Wei Gong
Yimeng Huang
Jia Zhao
Jiangchuan Liu

Pervasive Ambient Communication for Internet of Things

Springer

Pervasive Ambient Communication for Internet of Things

Wei Gong • Yimeng Huang • Jia Zhao •
Jiangchuan Liu

Pervasive Ambient Communication for Internet of Things

Springer

Wei Gong
University of Science and Technology of China
Hefei, China

Yimeng Huang
University of Science and Technology of China
Hefei, China

Jia Zhao
Simon Fraser University
Burnaby, BC, Canada

Jiangchuan Liu
Simon Fraser University
Burnaby, BC, Canada

ISBN 978-3-031-38043-3 ISBN 978-3-031-38044-0 (eBook)
https://doi.org/10.1007/978-3-031-38044-0

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Little sparks light great fires.

—While pervasive ambient backscatter is at its infancy stage, we firmly believe that as more and more passionate individuals join, it will become one of the dominating technologies for future IoT applications.

Foreword

We are now in an era where wireless connectivity is ubiquitous. The potential of this comprehensive exploration of ambient backscatter communications to revolutionize the Internet of Things (IoT) is both timely and extraordinary. The notion of communication has taken on a new dimension—one that surpasses traditional means and permeates our surroundings. Welcome to the world of pervasive ambient communication.

The concept of pervasive ambient communication is rooted in the idea that communication should be integrated seamlessly into our surroundings. It emphasizes the importance of creating environments that are not only aware of our presence but also responsive to our needs. As we navigate an increasingly interconnected society, the exchange of information has transcended the constraints of mere devices and screens. Through innovative technologies and intelligent systems, pervasive ambient communication aims to enhance human interaction, facilitate collaboration, and create a harmonious fusion between the physical and digital realms.

This monograph offers a visionary perspective on pervasive backscatter communication for IoT. In this monograph, the authors expertly depict the state-of-the-art ambient backscatter techniques, shedding light on the remarkable progress achieved thus far in this field. From its insightful introduction to the exploration of ambient backscatter techniques and the unveiling of advanced methodologies, they illuminate the path toward achieving pervasive backscatter. Throughout the chapters, they navigate the complexities and implications of achieving pervasive backscatter communication, delving into innovative methodologies, cutting-edge technologies, and novel approaches. By charting the future directions and possibilities, this book inspires readers to push the boundaries of innovation and realize the full potential of ambient backscatter in the IoT landscape. Their work represents a significant leap forward in harnessing the potential of ambient backscatter to establish seamless connections among IoT devices.

I find the monograph enjoyable to read and fully recommend it to you. It is my sincere hope that this monograph will catalyze further exploration, innovation, and

the realization of a future where pervasive ambient communication enhances our lives in ways we have yet to imagine.

Princeton, NJ, USA
May 2023

Chonggang Wang
Founding Editor-in-Chief, IEEE IoT Journal (2014–2016)
Steering Committee Chair, IEEE IoT Technical Community (2023–2025)

Preface

Pervasive Ambient Communication for the Internet of Things (IoT) refers to the seamless and pervasive connectivity between IoT devices and their ability to communicate with each other in various environments. By enabling pervasive ambient communication, the IoT ecosystem can support a wide range of applications and services, including smart homes, intelligent transportation systems, healthcare monitoring, industrial automation, and more. This communication paradigm facilitates the integration of IoT devices into everyday life, enabling them to work together harmoniously and autonomously, ultimately improving efficiency, convenience, and productivity. Ambient backscatter is one of the cutting-edge technologies that make this vision a reality. By harnessing the ambient radio signals that permeate our environment, IoT devices equipped with ambient backscatter capabilities can effectively communicate with each other without relying on traditional wireless transmission methods.

This monograph aims to provide an in-depth understanding of ambient backscatter technologies. In particular, we mainly take ubiquitous Wi-Fi signals as the communication sources and adopt a top-down approach to introduce three crucial subjects: Wi-Fi backscatter communication, ambient backscatter network, and self-powered application systems. For each subject, we carefully divide it into several relatively independent topics, which come with the latest advances in pervasive backscatter and include extensive discussions of closely related state-of-the-art methodologies.

This monograph will cover several essential aspects of pervasive ambient backscatter communication, one of the most cutting-edge technologies for Internet of Things. It begins with introductory Part I, which presents visions, basic concepts, principles, and paradigms of ambient backscatter. Also, a taxonomy of state-of-the-art ambient backscatter systems is provided from the perspective of the OSI model. Part II and III study how ambient backscatter systems work on the communication and networking levels. Specifically, Part II discusses in detail how to make use of ambient Wi-Fi signals to provide high-throughput backscatter communications with Wi-Fi 1 (Chap. 5), Wi-Fi 2–3 (Chap. 4), Wi-Fi 4 (Chap. 3), and Wi-Fi 5–6 (Chap. 6) standards. Further, Part III includes several of the most advanced

ambient backscatter network solutions, which are made possible by the first multi-hop backscatter (Chap. 7), first backscatter mesh (Chap. 8), and multiprotocol backscatter (Chap. 9). On top of reliable communication and networks, we propose two novel applications that are thought impossible before, lightweight spatial sound recording over the air (Chap. 10), and self-powered wireless wearables for healthcare (Chap. 11). To conclude the monograph, we point out critical challenges for realizing the vision of pervasive backscatter IoTs and potential directions of ambient backscatter applications.

We believe this monograph will inspire more efforts from and outside the IoT research community and will significantly contribute to the fast development of interdisciplinary research areas, such as smart healthcare, smart homes, and intelligent logistics.

Anticipated Audience

The prominent feature of this monograph is to provide state-of-the-art research technologies, ideas, and outcomes in ambient backscatter areas, which are trending and hot topics in the IoT community. The primary audience would be scientists and researchers in pervasive computing and IoT. We expect the audience with EECS-related bachelor degrees or equivalent can grasp most of the contents. We also hope technicians and practitioners from the IoT industry will gain the latest knowledge from those academic works and draw attention to translating those advanced techniques and prototypes into real-world products, making us a better world. For students, engineers, and researchers who are not familiar with backscatter, we anticipate this monograph can provide interesting ideas and motivate them to use, research, or apply pervasive backscatter technologies in a world of interconnected smart things.

Hefei, China — Wei Gong
Hefei, China — Yimeng Huang
Burnaby, BC, Canada — Jia Zhao
Burnaby, BC, Canada — Jiangchuan Liu
May 2023

Acknowledgements

In the course of working on pervasive ambient communication research in recent years, we have been immensely fortunate to receive invaluable support and assistance from our circle of friends and colleagues. With deep appreciation, we would like to seize this opportunity to express our sincerest gratitude to them.

We are indebted to the diligent efforts of the students in the UBIoT at USTC, who have contributed their time and expertise to the editing process of this monograph. They include Longzhi Yuan, Yunyun Feng, Yifan Yang, Weiqi Wu, Jiuwei Li, Lijie Liu, Yun-Hao Liu, Xinyue Lu, Zhaoyuan Xu, and Zhanxiang Huang.

In this monograph, we delve into the forefront of an academic discipline on ambient backscatter. Here we would like to particularly thank Shyamnath Gollakota, Joshua Smith, Pengyu Zhang, and Deepak Ganesan for their pioneering work in the relevant fields. We appreciate much help and inspiration from well-known wireless communication and networking researchers, including Sherman Shen and Ivan Stojmenovic. We are also grateful to the editors of Springer, especially Susan Grove, Kala P, Kate L and Shanthini K, for their continuous professional support and guidance.

We would like to acknowledge the support from the NSFC for their long-term project funding. Thanks must also go to USTC for the start-up grant support. Without their funding for our research, it would be hard to construct forward-looking research results in this monograph.

Finally, we would like to express our thanks to the family of each of us for their persistent and selfless support. We affectionately dedicate this book to them.

Contents

Part I Background

1 Vision of Pervasive Backscatter 3
1.1 What Is Backscatter Communication 3
1.2 Basic Concepts of Pervasive Backscatter 5
1.3 Pervasive Backscatter for IoTs 7
References 9

2 Understanding State-of-the-Art Ambient Backscatter 11
2.1 Pervasive Backscatter Characteristics 11
2.1.1 Uplink and Downlink 11
2.1.2 Network for Backscatter 12
2.2 State-of-the-Art Backscatter Systems 13
2.3 Critical Challenges 16
2.3.1 Efficiency of Tag Data Transmission 16
2.3.2 Compatibility of Commodity Excitor and Receiver 17
2.3.3 Identification of Target Carriers 18
References 19

Part II Backscatter Communication with Ambient Excitations

3 Spatial Stream Backscatter with Multiplexing Wi-Fi 25
3.1 Introduction 25
3.2 Related Work 28
3.3 Codeword Translation for Spatial Stream Wi-Fi 29
3.3.1 Spatial Stream Wi-Fi Primer 29
3.3.2 Tag Codebook Design for Advanced Wi-Fi 31
3.4 MOXcatter Design 33
3.4.1 Wi-Fi Signal Detector 33
3.4.2 Tag Modulation 35
3.4.3 Tag Information Decoding 36
3.4.4 Control Signals 38

3.4.5 Symbol-Level Modulation in Multi-Stream Wi-Fi 39
3.5 Performance Evaluation 40
3.5.1 Implementation and Setup 40
3.5.2 Evaluation 41
3.6 Application Case 44
3.7 Discussion 45
3.7.1 Throughput Enhancement 45
3.7.2 Dual Receivers 46
3.7.3 Multiple Access Control 46
3.8 Summary 46
References 47

4 Single-Symbol Wi-Fi Backscatter with Uncontrolled Ambient Signals 49
4.1 Introduction 49
4.2 Related Work 51
4.3 Wi-Fi Backscatter Background 52
4.3.1 OFDM Wi-Fi 52
4.3.2 Codeword Translation 53
4.4 RapidRider Design 53
4.4.1 Overview 53
4.4.2 Single-Symbol Modulation 54
4.4.3 Deinterleaving Decoding 57
4.4.4 Deinterleaving-Twins Decoding 57
4.5 RapidRider+ Design 59
4.5.1 Single-Receiver for Aggregated Transmissions 59
4.6 Performance Evaluation 60
4.6.1 Implementation 60
4.6.2 Evaluation 61
4.7 Application Case 68
4.7.1 Office Check-In 68
4.7.2 Railway Inspection 68
4.8 Summary 68
References 69

5 Symbol and Sub-Symbol Wi-Fi Backscatter for 802.11b 71
5.1 Introduction 71
5.2 Related Work 74
5.2.1 Backscattering with COTS Radios 74
5.2.2 Codeword Translation 74
5.2.3 Smart Community 75
5.3 802.11b Wi-Fi Primer 75
5.3.1 802.11b Wi-Fi Packet Format 75
5.3.2 Low Rate DSSS Transmission 76
5.3.3 High Rate CCK Transmission 76
5.4 Symbol Level Modulation Design 76

5.4.1 Overview 76
5.4.2 Codeword Translation and Symbol Level Modulation ... 77
5.4.3 CRC Reverse Decoding 78
5.5 Sub-Symbol Level Modulation Design 82
5.5.1 Overview 82
5.5.2 Sub-Symbol Modulation 83
5.6 Performance Evaluation 88
5.6.1 Implementation 88
5.6.2 Evaluation 91
5.7 Application Case 97
5.8 Summary 99
References 99

6 Content-Agnostic Backscatter with Ambient OFDM Signals 103
6.1 Introduction 103
6.2 Related Work 105
6.3 Background 106
6.3.1 Ambient Backscatter System 106
6.3.2 Basic Idea 106
6.4 CAB Design 108
6.4.1 Overview 108
6.4.2 Tag-Data Demodulation 108
6.4.3 Ambient-Data Demodulation 112
6.4.4 Subsymbol-Level Synchronization 113
6.5 Performance Evaluation 115
6.5.1 Implementation 115
6.5.2 Evaluation 116
6.6 Application Case 121
6.6.1 Smart Agricultural 121
6.7 Discussion and Future Work 122
6.7.1 COTS Receiver 122
6.7.2 Ambient Traffic Patterns 122
6.7.3 QAM Modulation 123
6.8 Summary 123
References 123

Part III Towards Backscatter Networks at Scale

7 Multi-Hop Wi-Fi Backscatter 129
7.1 Introduction 129
7.1.1 Motivation and Background 129
7.1.2 Challenges 130
7.1.3 Solutions 132
7.2 Related Work 133
7.3 Wi-Fi PHY Primer 134
7.4 System Design 135

7.4.1 Transmitter Side 135
7.4.2 Tag Side 136
7.4.3 Receiver Side 141
7.5 Performance Evaluation 143
7.5.1 Implementation Details 143
7.5.2 Experimental Results 145
7.6 Application Case 151
7.6.1 Health Care 151
7.6.2 Autonomous Vehicles 152
7.7 Summary and Discussion 152
References 153

8 Multi-Hop Backscatter Sensor Mesh 157
8.1 Introduction 157
8.2 Related Work 160
8.3 Multi-Hop Backscatter Communication Background 162
8.4 Design 162
8.4.1 Overview 162
8.4.2 Sensing Path 163
8.4.3 Relay Path 165
8.4.4 Simultaneous Backscatter for Two Paths 167
8.4.5 Reader Demodulation 168
8.4.6 Relay Mode and Reconfiguration of Tags 168
8.5 Performance Evaluation 168
8.5.1 Implementation 168
8.5.2 Evaluation 173
8.6 Application Case 182
8.6.1 Location Management 182
8.6.2 Patient Information Monitoring 183
8.7 Summary 183
References 184

9 Multiprotocol Backscatter with Commodity Radios 187
9.1 Introduction 187
9.2 Related Work 190
9.3 Multiscatter Design 191
9.3.1 Overview 191
9.3.2 High-Bandwidth Signal Acquisition 192
9.3.3 Low-Power Protocol Identification 194
9.3.4 Overlay Modulation 197
9.3.5 Event-Driven State Machine 200
9.4 Performance Evaluation 202
9.4.1 Implementation 202
9.4.2 Evaluation 203
9.5 Application Case 209
9.5.1 Personal Health Monitoring 209

9.6 Summary 210
References 210

Part IV Innovative Backscatter-Enabled Applications

10 Microphone Array Backscatter 215
10.1 Introduction 215
10.2 Related Work 219
10.3 Microphone Array Backscatter Design 220
10.3.1 Audio Modulation 220
10.3.2 Backscatter Transmission 223
10.3.3 Audio Regeneration 225
10.3.4 Hardware Customization 226
10.4 Evaluation 227
10.4.1 Implementation 228
10.4.2 Quality of Service 230
10.4.3 Coverage 232
10.5 Application 234
10.5.1 Acoustic Imaging 234
10.5.2 Spatial Filtering and Speech Enhancement 235
10.5.3 Ultrasonography 236
10.6 Discussion 237
10.7 Summary 239
References 240

11 Apollo: Battery-Free Wearable Sweat Monitoring System 245
11.1 Introduction 245
11.2 Related Work 248
11.3 Apollo Design 248
11.3.1 System Overview 248
11.3.2 Backscatter Communication 249
11.3.3 Power Management 253
11.3.4 Energy-Efficient Sweat Sensing 255
11.4 Performance Evaluation 256
11.4.1 Implementation Details 256
11.4.2 Evaluation Results 258
11.5 Application Case 262
11.5.1 Disease Diagnosis 262
11.5.2 Athlete Health Monitoring 263
11.6 Summary 263
References 263

Part V Future Directions

12 Challenges and Applications of Pervasive Backscatter 269
12.1 Urgent Challenges 269
12.2 Large-Scale Applications 271
References 273

Acronyms

ADC	Analog-to-Digital Converter
AFE	Analog Front End
AP	Access Point
ASIC	Application-Specific Integrated Circuit
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CCK	Complementary Code Keying
CDF	Cumulative Distribution Function
CSI	Channel State Information
CW	Continuous Wave
DC	Direct Current
DCM	Digital Clock Manager
DPPM	Differential Pulse Position Modulation
DRX	Discontinuous Reception
DS	Double Streams
DSSS	Direct Sequence Spread Spectrum
ENOB	Effective Number of Bits
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FPGA	Field-Programmable Gate Array
GI	Gastrointestinal
GFSK	Gaussian Frequency-Shift Keying
HT	High Throughput
IDFT	Inverse Discrete Fourier Transform
IFF	Identification Friend or Foe
IFFT	Inverse Fast Fourier Transform
IoT	Internet of Things
ISM	Industrial Scientific Medical
LED	Light-Emitting Diode
LOS	Line of Sight
LTF	Long Training Field

MC	Mesh Client
MCS	Modulation Coding Scheme
MFS	Multiple Frequency Shifts
MG	Mesh Gateway
MIMO	Multiple Input Multiple Output
MIT	Massachusetts Institute of Technology
MR	Mesh Router
NIC	Network Interface Card
NLOS	Non-Line of Sight
OFDM	Orthogonal Frequency-Division Multiplexing
PARP	Peak-to-Average Power Ratio
PER	Packet Error Rate
PLCP	PHY Layer Convergence Procedure
PPDU	PLCP Protocol Data Unit
PPM	Pulse Position Modulation
PSK	Phase Shift Keying
PSNR	Peak Signal-to-Noise-Ratio
PSS	Primary Synchronization Signal
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indicator
SDR	Software-Defined Radio
SFD	Start Frame Delimiter
SHM	Structural Health Monitoring
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SPST	Single-Pole Single-Throw
SQNR	Signal-to-Quantization Noise Ratio
SS	Single Stream
SSS	Secondary Synchronization Signal
STBC	Space-Time Block Coding
STF	Short Training Field
TEG	Thermoelectric Generator
WMN	Wireless Mesh Network
WSN	Wireless Sensor Networks

Part I
Background

Part I presents two chapters. In the first chapter, we briefly review the history of backscatter communication and then introduce the basic concepts of the pervasive backscatter mechanism. We also discuss the advantages of pervasive backscatter, demonstrating it is one of the most promising techniques for realizing IoTs.

In Chap. 2, we first introduce key characteristics of pervasive backscatter communication. Then we provide a taxonomy of state-of-the-art backscatter systems from the perspective of excitations and discuss their pros and cons. Finally, we outline several critical issues to make ambient backscatter systems practical.

Chapter 1
Vision of Pervasive Backscatter

Abstract This chapter presents visions, basic concepts, principles, and paradigms of ambient backscatter in detail. The reader can get an initial understanding of ambient backscatter, such as exploring its development and origin from history, understanding its working mechanism from basic concepts, and discovering potential applications based on its features.

1.1 What Is Backscatter Communication

Backscatter communication is one of the most essential technologies for Internet of Things (IoT) as it can provide ubiquitous connectivity to ultra-low-power sensors. Radio Frequency Identification (RFID) is in widespread use worldwide and is the most popular backscatter communication. Figure 1.1a shows the history of RFID [1]. RFID originated during World War II. Discovered by Sir Robert Alexander Watson-Watt in 1935, radar is widely used in the American, British and German armies. However, the radar signatures used to detect incoming aircraft cannot tell which planes belong to the enemy and which belong to their own forces. Later, the Germans discovered that if pilots taxied their planes as they returned to base, this would change the reflected radar signal and thus roughly determine whether it was enemy or friendly. The British took this idea a step further and invented the Identification Friend or Foe (IFF) system, which consisted of transmitters mounted on each aircraft that responded to radar broadcast signals to indicate that the aircraft was friendly. In 1945, Leon Theremin was inspired to develop a Soviet spy tool called The Thing that used RFID-like technology. Theremin created a musical instrument that can be played without physical contact due to the static frequency waves it produces. Inspired by this, the Soviet Union concealed an antenna activated by radio waves in the gift medal sent to the US ambassador. The seals then transmitted audio from the surrounding area back to the Soviet Union. Because it required no batteries or wires, the device sat undiscovered in the ambassador's study for a full seven years. It wasn't until 1973 that the first RFID patent was awarded to Mario W. Cardullo, who created an active RFID tag system using rewritable memory. That same year, Charles Walton received a patent

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_1

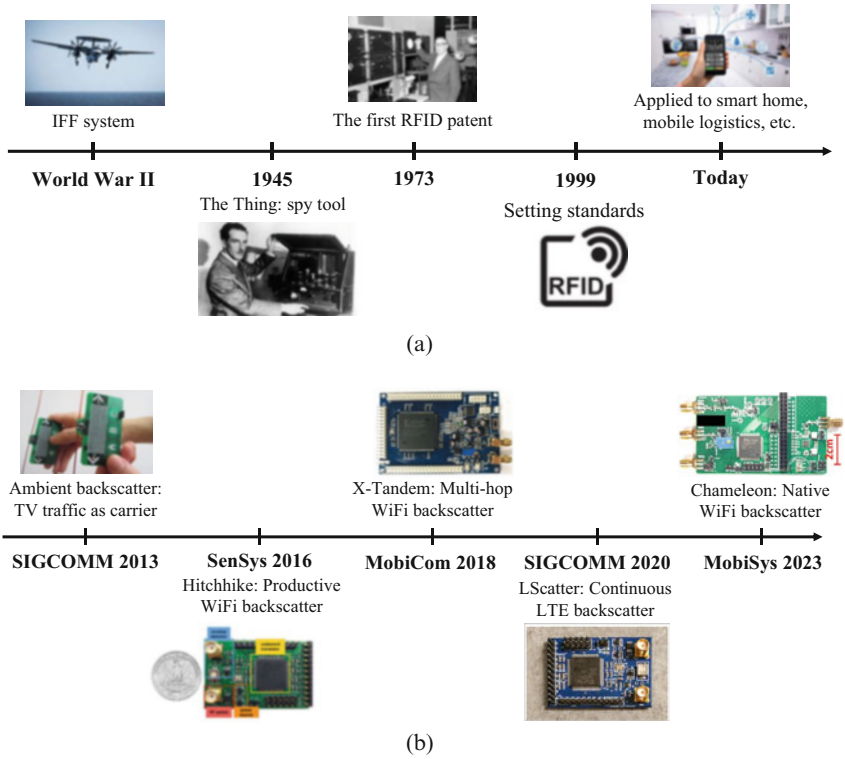


Fig. 1.1 Backscatter communication history. (**a**) History of RFID. (**b**) History of pervasive backscatter

for a passive RFID system, designing a passive transponder that would allow the door to be opened without a key. RFID was given a further boost in 1999 when scientists at the Massachusetts Institute of Technology (MIT) founded the Auto-ID Center to standardize the format of RFID-encoded information. To make RFID a viable solution for supply chains and other industries, the Auto-ID Center was committed to reducing its production costs. With the maturity of RFID technology, it has been widely used, involving all aspects of social life, and can be applied in logistics, retail, the clothing industry, medical treatment, identification, anti-counterfeiting, asset management, transportation, food, military, financial payment, and other fields. RFID has a significant effect on improving enterprise operating efficiency and reducing operating costs. At present, it is rapidly promoted in the fields of financial payment, identification, traffic management, and logistics.

Nevertheless, the requirement for expensive and dedicated RFID readers makes backscatter systems extremely difficult to deploy on a large scale. As a result, the researchers explored ambient backscatter using existing infrastructure and commercial radios. Figure 1.1b shows the history of pervasive backscatter. Ambient backscatter [2] proposes to use ambient TV traffic as an excitation signal for the

first time, which provides a new idea for backscatter networks and opens the door for backscatter transmission [3–8] using ambient signals as carriers. FS backscatter [9] observes that frequency shift is the key to improving the communication quality of backscatter transmission. Although BackFi [10] achieves high throughput, it uses full-duplex radios to cancel self-interference from excitation sources, which is not possible with existing devices. To make backscatter work with commercial devices, passive Wi-Fi [11] uses plugged-in devices to transmit a single-tone signal outside the desired Wi-Fi channel. This idea is also used in BLE backscatter and LoRa backscatter [7]. But these works require dedicated hardware to send single-tone signals. To do this, Interscatter [12] uses a Bluetooth device to generate a single-tone signal to create Wi-Fi- and ZigBee-compatible signals. However, inverse whitening prohibits the productive signal from being used as a carrier. Hitchhike [4] is the first to propose a productive carrier to work with commercial devices. FreeRider [3] and MOXcatter [13] follow this idea. X-Tandem [14] enables multi-hop backscatter that works with commercial Wi-Fi devices. RBLE [15] presents a BLE backscatter system communicating with a single receiver. Nevertheless, these works use bursty and intermittent ambient signals as carriers, making the backscatter communication unstable. The first LTE backscatter system, LScatter [16] proposes ubiquitous and high-throughput backscatter communications using LTE signals. Unfortunately, none of the existing Wi-Fi backscatter works can backscatter the productive carrier into native Wi-Fi packets received by COTS Wi-Fi devices since they require specific excitation patterns or software/hardware modifications to the receiver. Chameleon [17] enables tags to generate native Wi-Fi packets using uncontrolled productive carriers. The key insight is that the Chameleon tag can demodulate the Wi-Fi signal.

1.2 Basic Concepts of Pervasive Backscatter

We first introduce the principles of RFID and pervasive backscatter, and then introduce the difference between the two from three aspects.

As shown in Fig. 1.2a, a typical RFID system includes two types of devices, readers and tags. The reader sends continuous wave, and the tag receives the RF signal from the reader and generate an induced current. With the energy generated

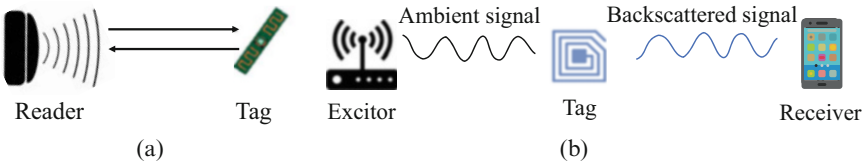


Fig. 1.2 The principles of RFID and pervasive backscatter. (**a**) The principle of RFID. (**b**) The principle of pervasive backscatter

by this current, the tag powers itself and then modulates the RF signal back to the reader by adjusting the impedance matching on its antenna. Specifically, the tag sends a bit one by changing its antenna impedance to reflect the wave, and a bit zero by just keeping in the silent state. After receiving the information returned by the tag, the reader decodes it.

As shown in Fig. 1.2b, pervasive backscatter consists of three different types of devices, excitor, tag and receiver. Both the excitor and the receiver are commercial radio devices. The ambient signal emitted by the excitation source is used as the carrier. To transmit data, the tag reflects the excitation signal from the excitor, changing the amplitude, frequency or phase of the signal. The receiver captures the backscattered signal to extract the information embedded by the tag.

The difference between RFID and pervasive backscatter is mainly reflected in the following three aspects.

(1) Excitor and Receiver. The RFID reader acts as both the carrier provider and receiver. Although the dual-role design reduces system complexity, the high cost prevents its mass adoption in everyday use. Because it requires expensive and dedicated equipment and cannot reuse existing commercial radio infrastructures. Pervasive backscatter is different, its excitor and receiver are two different devices. Taking Wi-Fi backscatter as an example, the excitor can be a router, and the receiver can be a mobile phone. These radio devices are all over the surrounding environment. We don't need customized hardwares, but use existing radio devices to meet the transceiving requirements of pervasive backscatter. This reduces cost and deployment difficulty considerably. In addition, the excitation signal can be various, for example, RF signal including Wi-Fi, Bluetooth, and LTE, optical signal and acoustic signal. This provides an opportunity for pervasive backscatter to realize multi-protocol data transmission, avoiding the communication failure issue of the single-protocol backscatter system in the absence of carriers, and greatly improving the system transmission efficiency.

(2) Tag. On the one hand, RFID tags have been chip-based, and UHF RFID tag chips have a history of nearly 20 years. There have been various innovations in the development process, from the early pursuit of sensitivity (before 2010) to the pursuit of multiple innovative functions (2010 to 2015), until now the main pursuit of cost and stability (2015 to 2020). The world's representative RFID chip suppliers include Impinj, NXP, and Alien, which promote the miniaturization and higher sensitivity of tag chips. The tag for pervasive backscatter is still in the prototype stage and has not yet been chipped. On the other hand, RFID uses encryption technology considering security and privacy concerns. This technology has been widely used, such as document anti-counterfeiting and traffic ticket inspection. The tags of pervasive backscatter do not use encryption technology.

(3) Protocols. RFID uses well-established protocols, for example, UHF RFID uses the EPC C1G2 standard, which contains different layers that define the communication between the reader and the tag. Pervasive backscatter supports a

variety of mainstream radio protocols, including Wi-Fi, LTE and 5G. Moreover, these protocols are being updated all the time. Let's take Wi-Fi as an example. Wi-Fi is based on IEEE 802.11. In 1999, IEEE launched two protocols, 802.11a and 802.11b. With the popularization of Wi-Fi, people have higher and higher requirements for wireless transmission rate. By 2003, the 802.11g protocol was applied. In 2008, Wi-Fi 4 based on 802.11n made a major change and introduced MIMO technology. By 2014, Wi-Fi 5 with 802.11ac as the standard was launched, providing higher data transfer rates. In 2019, Wi-Fi 6 with 802.11ax as the standard was launched, which further improved the data transmission rate and the connection efficiency of devices. To this day, Wi-Fi standards continue to develop and evolve.

1.3 Pervasive Backscatter for IoTs

The ultimate goal of IoT is the Internet of Everything, allowing any item in our physical world, even a speck of dust, to be remotely sensed or controlled. For example, with IoT sensors, a farmer could remotely monitor nutrition levels in a field, and fertilize those withered crops at the right time. By deploying IoT sensors on each item, a warehouse manager could remotely identify, count or categorize every item in the large warehouse without the need to manually inventory each of them.

Compared with active radio, backscatter radio does not need to generate a carrier, and has advantages such as ultra-low power consumption and low cost, which make it a desirable alternative for active radio. Although RFID also has the characteristics of low power consumption as a backscatter technology, it still cannot be deployed on a large scale due to the need for expensive and dedicated hardware that increases the cost and complexity of deployment. Pervasive backscatter is one of the best ways to realize IoT backscatter because of its features as shown in Fig. 1.3.

(1) Battery-free. Because pervasive backscatter does not need to generate a carrier and uses passive circuit components, its power consumption is extremely low, at the microwatt level. Compared with active radios, pervasive backscatter radios consume orders of magnitude lower power. Such a design can significantly prolong the service life of tags and reduce maintenance risks and costs. Specifically, it is well suited for applications where battery replacement is challenging and long battery life is required. To further reduce power consumption, some research uses the wake-up mechanism to avoid continuous sensing and transmission. When the tag is not in the working state, it will enter the sleep state to save power. To achieve a completely battery-free approach, the researchers propose combining backscatter and energy harvesting. The tag captures the energy in the environment through the energy harvester, including RF energy, light energy and thermal energy, and then converts these energies into electrical energy for tag communication. The battery-free feature of pervasive backscatter

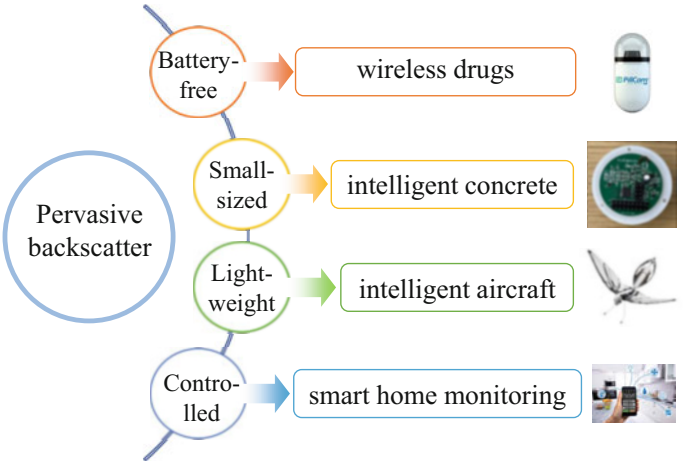


Fig. 1.3 Features of pervasive backscatter

can be used in various applications, such as wireless drugs. We know that human tissue is much more complex than air, making some pathologies tricky to detect and treat. If pervasive backscatter is applied to medicine, on the one hand, no need to replace the battery allows the drug to have a longer service life to sense and transmit the health status of the human body; on the other hand, we can use the wireless drug to locate the lesion area and make treatment.

(2) **Small-sized.** To meet various application requirements, tags are required to be miniaturized. Miniaturized tags are achievable. On the one hand, the logic of the tag is simple, and it is mainly used to sense and transmit a small amount of data. As a result, the circuit design of the tag is also simple. On the other hand, mature manufacturing processes and advanced materials provide support for tag miniaturization. Small-sized tags can be used in some space-constrained and privacy-safe applications. For example, for structural health monitoring (SHM) of the buildings, sensors measure variations in parameters, such as acoustic emission, temperature, strain, force, pressure, or acceleration. Traditional sensing solutions for SHM include the use of fiber optical sensors, electrochemical sensors, and piezoelectric sensors, but these methods require wired connections, making the sensor size too large for deployment. To solve this issue, miniaturized wireless sensors can be used in SHM, by mixing the sensors into the concrete to monitor the internal performance of the building and using backscatter to transmit this data.

(3) **Lightweight.** In addition to requiring miniaturization, there are also some applications that require the sensor to be very light, especially those with limited load capacity. To realize the lightweight sensor, the circuit of the tag is integrated as much as possible. In addition, wireless connections are necessary to replace wired connections. This lightweight sensor can be used for military reconnaissance. With the development of sensing technology, the demand for

sensing in the field of national defense and military is getting higher and higher. The sensors used in traditional military reconnaissance are mainly wired for power supply and data acquisition, which undoubtedly increases the weight of the sensor, and even the use of batteries further increases the weight. Military reconnaissance often requires concealment so that it is not easy to be discovered by the enemy. Some researches have made the reconnaissance equipment into the appearance of insects, flying in the air to detect the enemy's situation, which has to require that the weight of the aircraft is quite light enough to carry the entire sensor. Obviously, wireless passive sensing greatly reduces the weight of the sensor due to the elimination of wired connections and the absence of batteries. Therefore, pervasive backscatter sensors are more suitable for military reconnaissance.

(4) Controlled. Sensors can be used for sensing and transmission, and can be widely used in various IoT applications, such as smart home, mobile medical, and smart logistics. Taking indoor temperature monitoring for fire prevention in smart homes as an example, first of all, the demand for temperature monitoring is controlled, because the possibility of fire in different places and time periods is different. For example, kitchens are more prone to fires than bedrooms, and fires occur more frequently in winter and spring than in summer and autumn. As a result, fire-prone places such as kitchens need to deploy more temperature sensors and sensors should spend more time monitoring indoor temperature in winter and spring. Other locations and time periods that are not prone to fire can reduce the number of sensor deployments and the duration of monitoring. Therefore, we can control sensor sensing and monitoring at an appropriate time and place according to monitoring needs, rather than at any time and place, which can not only speed up data processing, but also reduce the interference of other irrelevant data.

References

1. Landt, J (2005) The history of RFID. IEEE Potentials 24(4):8–11
2. Liu V, Parks A, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. In: Proceedings of ACM SIGCOMM
3. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of ACM CONEXT
4. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of ACM SenSys
5. Li Y, Chi Z, Liu X, Zhu T (2018) Passive-zigbee: enabling zigbee communication in IoT networks with 1000x+ less power consumption. In: Proceedings of ACM SenSys
6. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) PLoRa: a passive long-range data network from ambient LoRa transmissions. In: Proceedings of ACM SIGCOMM
7. Talla V, Hessar M, Kellogg B, Najafi A, Smith JR, Gollakota S (2017) Lora backscatter: enabling the vision of ubiquitous connectivity. In Proceedings of ACM IMWUT

8. Wang A, Iyer V, Talla V, Smith JR, Gollakota S (2017) FM backscatter: enabling connected cities and smart fabrics. In: Proceedings of USENIX NSDI
9. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of ACM SIGCOMM
10. Bharadia D, Joshi KR, Kotaru M, Katti S (2015) Backfi: high throughput wifi backscatter. In: Proceedings of ACM SIGCOMM
11. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In: Proceedings of USENIX NSDI
12. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In: Proceedings of ACM SIGCOMM
13. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of ACM MobiSys
14. Zhao J, Gong W, Liu J (2018) X-tandem: towards multi-hop backscatter communication with commodity wifi. In: Proceedings of ACM MOBICOM
15. Zhang M, Zhao J, Chen S, Gong W (2020) Reliable backscatter with commodity BLE. In: Proceedings of IEEE INFOCOM
16. Chi Z, Liu X, Wang W, Yao Y, Zhu T (2020) Leveraging ambient lte traffic for ubiquitous passive communication. In: Proceedings of ACM SIGCOMM
17. Yuan L, Gong W (2023) Enabling native wifi connectivity for ambient backscatter. In: Proceedings of ACM MobiSys

Chapter 2
Understanding State-of-the-Art Ambient Backscatter

Abstract This chapter provides a taxonomy of state-of-the-art ambient backscatter systems from the perspective of the OSI model. The Reader can gain a clear and in-depth understanding of the current state of research in the field of ambient backscatter.

2.1 Pervasive Backscatter Characteristics

Backscatter techniques have many distinctive characteristics compared with active radios, which will lead to unique network design. We first discuss the imbalanced uplink and downlink in backscatter, and then introduce its corresponding network design.

2.1.1 Uplink and Downlink

In active radio networks, the uplink and the downlink usually have similar characteristics and capabilities. For example, in Wi-Fi network, the *client* streams data to the *AP* by generating OFDM signals in a 20 or 40 MHz wireless channel. Similarly, *client* gathers information from the *AP* by resolving the same kind of signal [1].

On the contrary, backscatter has significantly imbalanced downlink and uplink capability. We take RFID as an example to explain this [2–4]. RFID tag contains a very simple envelope detector circuit that only reacts to signal amplitude for downlink reception. This means RFID support only ASK in the downlink. However, the RFID reader extracts exact the baseband signal using down-conversion components and precise ADC, making multiple modulations, such as ASK, PSK, and FSK, acceptable in the uplink. For such capacity imbalance, RFID has significantly different downlink and uplink modulations. In ISO 18000-6C (EPCglobal Class 1 Generation 2), the pulse-interval encoding (PIE) uses different intervals between negative pulses to convey data bits. As shown in Fig. 2.1, for bit '0', the interval equals to the pulse width, and their total length is defined as "Tari". When bit '1'

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_2

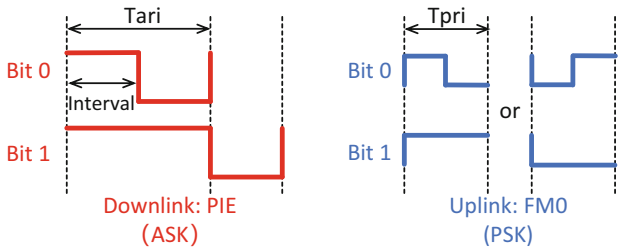


Fig. 2.1 The downlink and uplink for RFID in ISO 18000-6C

is to be transmitted, the PIE interval is larger than the pulse width. The reader can adjust the downlink rate between 40 and 160 kbps according to channel condition by choosing different Tari. The default uplink modulation is FM0. As shown in Fig. 2.1, it conveys bit '0' or '1' by choosing to invert the signal phase or not at the center of every symbol. The uplink rate ranges from 5 to 640 kbps.

In state-of-the-art backscatter systems, there is an even more significant imbalance between uplink and downlink [5–13]. The uplink has been the focus of research. Many modulation and demodulation methods have been designed to achieve better performance. For example, SubScatter [5] leverages complementary code keying (CCK) signal in 802.11b Wi-Fi as the backscatter carrier to realize an uplink throughput of 10.9 Mbps. TScatter [14] also achieves a throughput as high as 10 Mbps using OFDM signal as the carrier. However, on the other hand, there is very slow progress in backscatter downlink. The most common solution is using packet sizes to convey raw bits to backscatter tag [6]. For bits '1' and '0', packets with smaller and larger sizes will be generated, respectively. The corresponding data rate is less than 2 kbps. Interscatter [10] introduces using OFDM symbols to generate ASK signal directly and realizes a downlink throughput of about ∼100 kbps. But it is still much smaller than the uplink rate.

2.1.2 Network for Backscatter

Besides the uplink and downlink transmission methods, devices in a network also need to consider when and why to transmit and receive. The reader may be ordered to collect Electronic Product Code (EPC) codes of tags for inventory checking. It first Selects a tag. After that, EPC is collected to the reader through several commands shared in all ISO 18000-6C RFID systems, including "Query", "ACK", etc. The whole procedure is shown in Fig. 2.2. Those are defined in the RFID protocol for transmission control and are part of the RFID network. Similarly, the backscatter network should contain the data exchange method (PHY) and the transmission control mechanism (Link and MAC). We will introduce those aspects in backscatter networks.

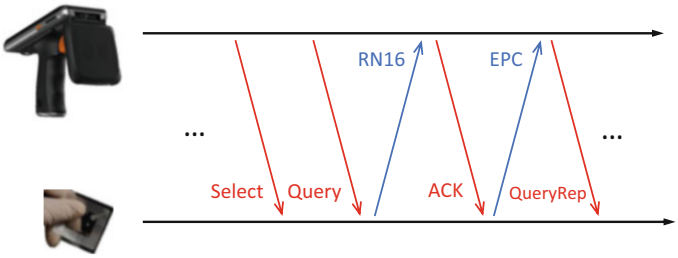


Fig. 2.2 The data exchange in a round of EPC collection

PHY Considering the imbalanced uplink and downlink, backscatter is usually used in areas where the uplink tasks are much heavier, such as electronic recognition and sensor data collection. Backscatter information is conveyed through electromagnetic wave. For downlink, active radios generate ASK signal for the tag. For uplink, the tag modulates the carrier wave to embed its data. The modulation method can be ASK, PSK, FSK, etc. The packet format, the data encoding method, and the backscatter modulation details should be defined in advance.

Link Backscatter should adapt its data rate according to the channel condition. When the channel is clear, a higher rate can be chosen. When the channel is busy, reliability becomes more important. Considering the capability imbalance between the reader and the tag, rate adaption is usually realized in the reader. Specifically, the reader can collect the backscattered signal and analyze the RSSI, frequency shift, phase shift, and other characteristics. Based on those, it can make the rate adaption decision. In this procedure, the reader can also adjust the adaption strategy according to the feedback on transmission performance.

MAC In typical backscatter scenarios, there exist a large number of tags. The backscatter network needs to control channel occupancy to avoid endless failure and retry. Considering the imbalance between uplink and downlink, tags are unable to monitor neighboring the channel and do the MAC control. Considering the tag population and the weak downlink, the management by the reader will take a long time and thus become inefficient. One proper solution may be ALOHA. The tag can randomly choose a time slot to transmit its data. If it gets the expected ACK from the reader, the transmission is successful. Otherwise, it will wait for a period and then start the introduced procedure again.

2.2 State-of-the-Art Backscatter Systems

State-of-the-Art (SoA) backscatter systems can be classified into four categories based on the types of their excitation and receivers, as shown in Fig. 2.3. Specif-

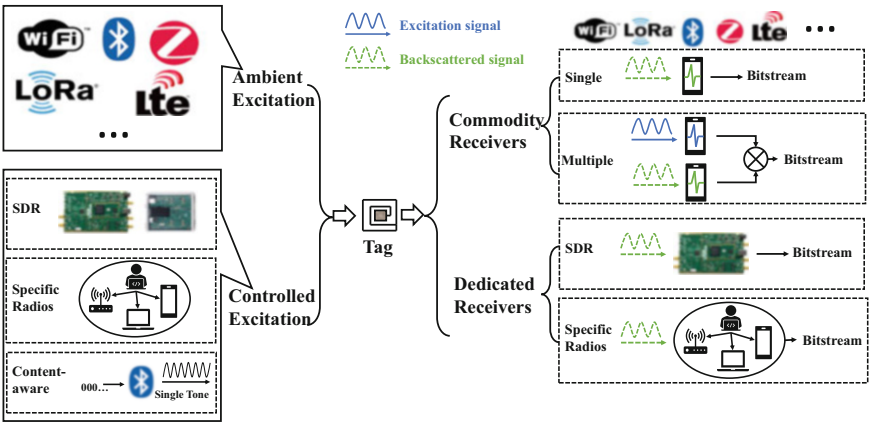


Fig. 2.3 Ambient excitation backscatter takes widely spread signals for the excitation, such as Wi-Fi, BLE, ZigBee, LoRa, LTE, . . . , .etc. Contrasting, controlled excitation backscatter takes signals from SDRs, specific radios, and content-aware radios for the excitation. Commodity or dedicated receivers are used to tag data

ically, ambient excitation involves utilizing signals that already present in the environment. These signals, such as Wi-Fi [15–20], BLE [17, 21], ZigBee [17, 22, 23], LoRa [24, 25], LTE [26, 27], and more, are widely spread and do not have any specific restrictions placed by the users. Contrastingly, controlled excitation refers to signals that users intentionally modify or restrict. This approach typically involves the use of software-defined radios (SDRs) [28–35], specific radios [36–42], or content-aware radios [43–47]. Users can employ either commodity receivers or dedicated receivers to decode tag data. On the one hand, if the backscattered signals are standard-compliant, commodity receivers can effectively decode tag data without requiring any significant modifications or redesigns of the wireless protocols [16–18, 20–25, 30, 36, 37, 41–47]. On the other hand, dedicated receivers are specifically designed and generally employ SDRs or specific radios for tag-data demodulation [15, 19, 26–29, 31–35, 38, 39]. These receivers may require a more comprehensive redesign of wireless protocols or modifications to existing protocols to achieve optimal performance. The detailed categories and their characteristics are described below.

(1) **Ambient excitation, commodity receivers:** Ambient excitation backscatter systems, specifically those utilizing commodity receivers, have been developed to enable tag-data demodulation without requiring modifications to existing radios. These systems leverage signals that are widely spread in the environment, such as Wi-Fi [16–18, 20], BLE [17, 21], ZigBee [17, 22, 23], LoRa [24, 25], and more. Users employ either multiple or single receivers for the tag-data demodulation. When it comes to multiple receivers, the user decodes the tag data through codeword translation [16–18, 27]. This involves using one receiver to decode ambient signals and another to decode backscattered signals.

The tag data is then decoded by comparing the differences between the two decoded signals. While this method allows for tag-data demodulation, it comes with increased deployment costs due to the need for multiple receivers. Another class focuses on achieving tag-data decoding using a single receiver [20–25]. These systems employ various techniques, such as modulating their own data based on the regularity observed in the decoded data at the receiver side or overwriting the original excitation information. By utilizing these innovative approaches, these systems aim to streamline the decoding process and reduce deployment costs associated with multiple receivers.

(2) **Ambient excitation, dedicated receivers:** Ambient excitation backscatter systems utilizing dedicated receivers have been developed to explore the underlying laws and characteristics of modulated signals that may not be fully supported by existing equipment. In order to access these unique features, researchers often rely on SDRs or dedicated devices with advanced developer capabilities, which may not available on mainstream models. While these dedicated receivers are not currently being widely adopted on a large scale, the investigation of these new features has generated significant interest. The potential for industry-academia integration in this field holds promising prospects for the future. Researchers are actively exploring the possibilities and implications of these advanced receivers, aiming to uncover valuable insights and advancements in the field of ambient excitation backscatter.

(3) **Controlled excitation, commodity receivers:** Controlled excitation backscatter systems utilizing commodity receivers aim to enhance the excitation source and minimize the decoding requirements at the receiving end. These systems strive to introduce new features to the excitation signals that may not be readily available or mandated by existing wireless protocols. Consequently, researchers need to implement these features using software radios or dedicated devices to overcome these limitations. In some cases, the content of the excitation source may need to be known to the tag for successful decoding. This requirement adds an additional dimension to the system design and necessitates mechanisms for the tag to acquire and process the excitation source information effectively. By leveraging commodity receivers, these controlled excitation backscatter systems offer the advantage of compatibility with widely available and standardized equipment. However, the introduction of new features and the need to address protocol limitations may require researchers to implement custom solutions using SDRs or dedicated devices.

(4) **Controlled excitation, dedicated receivers:** Controlled excitation backscatter systems utilizing dedicated receivers impose higher requirements on both the excitation source and the receiver, offering the potential to explore new features and capabilities. In this approach, a range of options are available for the excitation source, including SDRs, specific radios, or excitation sources with known content. Similarly, software radios or specific devices can be employed as receivers in these systems. The utilization of dedicated receivers enables researchers to delve deeper into the possibilities of controlled excitation backscatter. By employing SDRs, researchers can have greater flexibility and

control over the modulation and demodulation processes. Specific devices for backscatter systems further enhance the performance and customization options for the receiver. In addition, the choice of the excitation source becomes crucial in controlled excitation backscatter with dedicated receivers. Researchers can experiment with various options, including SDRs that offer programmability, specialized devices tailored to specific requirements, or even excitation sources with known content, allowing for more precise and targeted signal manipulation.

In summary, SoA backscatter systems can be categorized into four types: ambient excitation, controlled excitation with commodity receivers, controlled excitation with dedicated receivers, and controlled excitation with dedicated receivers. Each category offers distinct characteristics and considerations, enabling users to choose the most suitable approach based on their specific needs and constraints.

2.3 Critical Challenges

To enable a practical backscatter system, there are three critical challenges to overcome: efficiency of tag data transmission, compatibility of commodity excitor and receiver, and identification of target carriers.

2.3.1 Efficiency of Tag Data Transmission

Backscatter systems are mainly designed for low-power IoT applications like smart farms, health monitoring, and smart cities. Such applications require the efficiency of tag data transmission. Efficiency can be divided into three dimensions.

(1) Throughput. Throughput is defined as the amount of data that can be transferred per unit of time, which is an essential metric for a communication system. For some applications, like audio and video streaming, high throughput is necessary. To improve the throughput, there are two main challenges. First, how to harvest enough energy for such high throughput. Second, how to design a modulation method compatible with existing high-bandwidth protocols.

(2) Bit error rate. The bit error rate (BER) is defined as the percentage of error bits among all transmitted bits, which indicates the reliability of the communication system. Different from active radios, backscatter systems eliminate the use of high power-consumption components like Voltage-Controlled Oscillator (VCO), Power amplifiers (PA), and mixers. Instead of generating the high-frequency components, they backscatter excitation signals and embed their own data. The main problems are synchronization and modulation. First, to reduce power consumption, most backscatter systems use an energy detector for synchronization. In many cases, the simple synchronization method has low

accuracy, resulting in a high BER. Second, the tag modulates the signal by changing the impedance. How to make the backscatter signal compatible with the active radio is a challenge.

(3) **Power consumption.** Since the backscatter node needs to perform computation and communication tasks, it is a challenge to optimize its energy consumption. The challenge arises mainly in two areas: the low-power circuit design and the low power consumption algorithm design. First, design a low-power circuit, including the detector and modulation circuits. Second, design an algorithm using less computation and storage resources.

2.3.2 Compatibility of Commodity Excitor and Receiver

The second challenge is the compatibility of commodity excitor and receiver. The vision of ambient backscatter is to take advantage of the signals already in the environment and make the backscatter signals decodable to commercial devices. As Fig. 2.4 shows, there are plenty of commercial wireless devices in homes, cities and factories. Using the existing devices has two advantages. First, traditional systems like RFID use a dedicated RFID reader, which is bulky and expensive. Using existing infrastructure helps reduce the cost. Second, it makes the system available to a wide range of users. Using existing devices allows users to read tag information without having to purchase additional devices. But this is not an easy task.

First, low-power tags should identify different excitation signals and modulate accordingly, which will be further discussed in the next section. Second, making the backscatter signal compatible with different commercial standards is a challenge for both the physical layer and the upper layer. As different standards may use different modulation method, the tag should change the amplitude, phase, and frequency to meet different standards. And the upper layer stack, like MAC, is a challenge since the downlink ability of tags is relatively weak.

Fig. 2.4 Different commercial devices

2.3.3 *Identification of Target Carriers*

The identification of target carriers is important for two reasons:

(1) Availability in different environments. In different environments, the availability of signals is different. For example, Wi-Fi and Bluetooth signals are common in homes. But in the wild, LTE and 5G are more common. To make the system work in most scenarios, the tag should identify the signal and then modulate it accordingly.

(2) Different modulation methods. Different signals may have different modulation methods. As Fig. 2.5 shows, Bluetooth uses FSK modulation. Bluetooth uses low frequency to represent symbol 0 and high frequency to represent symbol 1. For Wi-Fi 802.11b, it is DBPSK. If the phase changes, the symbol is 1. Otherwise, the symbol is 0. For Zigbee, the modulation method is OQPSK. OQPSK modulates odd bits with I-way and even bits with Q-way. And the Q-way was delayed by one chip. To make the signal compatible with different modulation methods, we should first identify the signal. But the identification of target carriers is not easy. To reduce power consumption, low-power tags only use an envelope detector to detect the signal. It is a challenge to use simple energy information to distinguish between different excitation signals.

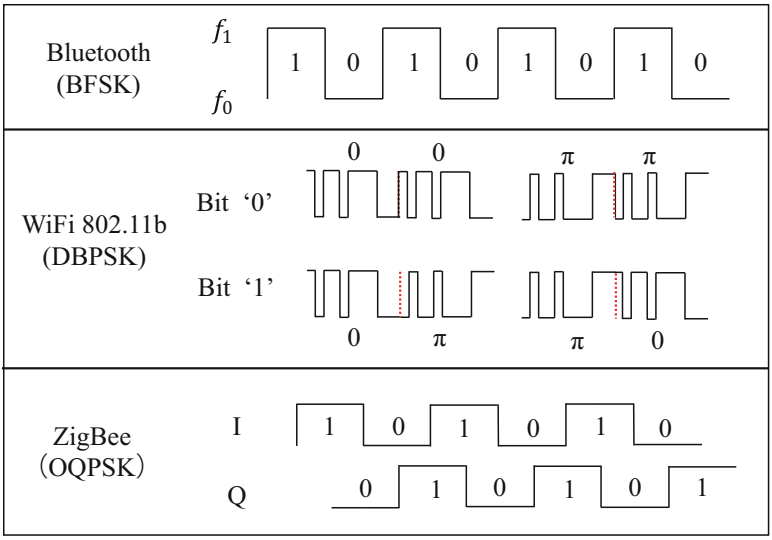


Fig. 2.5 Different modulation methods

References

1. IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: wireless lan medium access control (MAC) and physical layer (PHY) specifications (2012). In: IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007)
2. Dobkin D (2012) The RF in RFID: UHF RFID in practice. Newnes, Oxford
3. Gong W, Chen S, Liu J (2017) Towards higher throughput rate adaptation for backscatter networks. In: 2017 IEEE 25th international conference on network protocols (ICNP), pp 1–10
4. Gong W, Chen S, Liu J, Wang Z (2018) Mobirate: mobility-aware rate adaptation using phy information for backscatter networks. In: IEEE INFOCOM 2018 - IEEE conference on computer communications, pp 1259–1267
5. Yuan L, Gong W (2022) Subscatter: sub-symbol wifi backscatter for high throughput. In: 2022 IEEE 30th international conference on network protocols (ICNP), pp 1–11
6. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of the 13th international conference on emerging networking experiments and technologies, pp 389–401
7. Kellogg B, Parks A, Gollakota S, Smith JR, Wetherall D (2014) Wi-fi backscatter: internet connectivity for RF-powered devices. In: Proceedings of the 2014 ACM conference on SIGCOMM, pp 607–618
8. Bharadia D, Joshi KR, Kotaru M, Katti S (2015) Backfi: high throughput wifi backscatter. ACM SIGCOMM Comput Commun Rev 45(4):283–296
9. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In: 13th $\{USENIX\}$ symposium on networked systems design and implementation ($\{NSDI\}$ 16), pp 151–164
10. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In: Proceedings of the 2016 ACM SIGCOMM conference, pp. 356–369
11. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 370–383
12. Zhang P, Bharadia D, Joshi K, Katti, S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM, pp 259–271
13. Parks, AN, Liu A, Gollakota S, Smith JR (2014) Turbocharging ambient backscatter communication. ACM SIGCOMM Comput Commun Rev 44(4):619–630
14. Liu X, Chi Z, Wang W, Yao Y, Hao P, Zhu T (2021) Verification and redesign of OFDM backscatter. In: 18th USENIX symposium on networked systems design and implementation (NSDI 21), pp 939–953
15. Yang Y, Yuan L, Zhao J, Gong W (2022) Content-agnostic backscatter from thin air. In: Proceedings of the 20th annual international conference on mobile systems, applications and services, pp 343–356
16. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of ACM SenSys
17. Zhang P, Josephson C, Bharadia C, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of ACM CONEXT
18. Dunna M, Meng M, Wang PH, Zhang C, Mercier P, Bharadia D (2021) Syncscatter: enabling wifi like synchronization and range for wifi backscatter communication. In: Proceedings of USENIX NSDI
19. Liu X, Chi Z, Wang W, Yao Y, Zhu T (2020) Vmscatter: a versatile mimo backscatter. In: Proceedings of the 17th usenix conference on networked systems design and implementation (NSDI), pp 895–909

20. Kellogg B, Parks A, Gollakota S, Smith JR, Wetherall D (2014) Wi-fi backscatter: internet connectivity for RF-powered devices. In: Proceedings of the 2014 ACM conference on SIGCOMM, pp 607–618
21. Xu Z, Gong W (2023) Bumblebee: enabling the vision of pervasive zigbee backscatter communication. In: 2023 IEEE international conference on pervasive computing and communications (PerCom). IEEE, Piscataway, pp 252–261
22. Jung J, Ryoo J, Yi Y, Kim SM (2020) Gateway over the air: towards pervasive internet connectivity for commodity IoT. In Proceedings of the 18th international conference on mobile systems, applications, and services, pp 54–66
23. Li Y, Chi Z, Liu X, Zhu T (2018) Passive-zigbee: enabling zigbee communication in IoT networks with 1000x+ less power consumption. In Proceedings of ACM SenSys
24. Guo X, Shangguan L, He Y, Zhang J, Jiang H, Siddiqi AA, Liu Y (2020) Aloba: rethinking on-off keying modulation for ambient lora backscatter. In: Proceedings of ACM SenSys
25. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) PLoRa: a passive long-range data network from ambient LoRa transmissions. In: Proceedings of ACM SIGCOMM
26. Chi Z, Liu X, Wang W, Yao Y, Zhu T (2020) Leveraging ambient LTE traffic for ubiquitous passive communication. In: Proceedings of ACM SIGCOMM
27. Feng Y, Gong W (2022) LTE-like paging and synchronization for ambient backscatter. In: GLOBECOM 2022-2022 IEEE global communications conference, IEEE, Piscataway, pp 2038–2043
28. Naderiparizi S, Hessar M, Talla V, Gollakota S, Smith JR (2018) Towards battery-free HD video streaming. In: Proceedings of USENIX NSDI
29. Li S, Zhang C, Song Y, Zheng H, Liu L, Lu L, Li M (2020) Internet-of-microchips: direct radio-to-bus communication with SPI backscatter. In: Proceedings of the 26th annual international conference on mobile computing and networking, pp 1–14
30. Talla V, Hessar M, Kellogg B, Najafi A, Smith JR, Gollakota S (2017) Lora backscatter: enabling the vision of ubiquitous connectivity. In: Proceedings of ACM IMWUT
31. Hessar M, Najafi A, Gollakota S (2019) NetScatter: enabling large-scale backscatter networks. In: Proceedings of NSENIX NSDI
32. Zhao R, Zhu F, Feng Y, Peng S, Tian X, Yu H, Wang X (2019) OFDMA-enabled wi-fi backscatter. In: Proceedings of ACM MobiCom
33. Li S, Zheng H, Zhang C, Song Y, Yang S, Chen M, Lu L, Li M (2022) Passive {DSSS}: Empowering the downlink communication for backscatter systems. In: 19th USENIX symposium on networked systems design and implementation (NSDI 22), pp 913–928
34. Guo X, He Y, Yu Z, Zhang J, Liu Y, Shangguan L (2022) RF-transformer: a unified backscatter radio hardware abstraction. In: Proceedings of the 28th annual international conference on mobile computing and networking, pp 446–458
35. Song Y, Lu L, Wang J, Zhang C, Zheng H, Yang S, Han J, Li J (2023) {μMote}: enabling passive chirp de-spreading and {μW-level}{Long-Range} downlink for backscatter devices. In: 20th USENIX symposium on networked systems design and implementation (NSDI 23), pp 1751–1766
36. Li Z, Chen Y (2019) Achieving universal low-power wide-area networks on existing wireless devices. In: 2019 IEEE 27th international conference on network protocols (ICNP). IEEE, Piscataway, pp 1–11
37. Ensworth JF, Reynolds MS (2017) BLE-backscatter: ultralow-power IoT nodes compatible with bluetooth 4.0 low energy (BLE) smartphones and tablets. IEEE Trans Microwave Theory Techn 65(9):3360–3368
38. Zhu F, Feng Y, Li Q, Tian X, Wang X (2020) Digiscatter: efficiently prototyping large-scale OFDMA backscatter networks. In: Proceedings of ACM MobiSys
39. Katanbaf M, Weinand A, Talla V (2021) Simplifying backscatter deployment: full-duplex lora backscatter. In USENIX symposium on networked systems design and implementation (NSDI), pp 955–972

40. Rostami M, Chen X, Feng Y, Sundaresan K, Ganesan D (2021) MIXIQ: re-thinking ultra-low power receiver design for next-generation on-body applications. In: Proceedings of the 27th annual international conference on mobile computing and networking, pp 364–377
41. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In: Proceedings of USENIX NSDI
42. Abedi A, Dehbashi F, Mazaheri MH, Abari O, Brecht T (2020) WiTAG: seamless wifi backscatter communication. In: Proceedings of the annual conference of the ACM special interest group on data communication on the applications, technologies, architectures, and protocols for computer communication, pp 240–252
43. Zhang M, Zhao J, Chen S, Gong W (2020) Reliable backscatter with commodity BLE. In: Proceedings of IEEE INFOCOM
44. Zhang M, Chen S, Zhao J, Gong, W (2021) Commodity-level BLE backscatter. In: Proceedings of the 19th annual international conference on mobile systems, applications, and services, pp 402–414
45. Yuan L, Xiong C, Chen S, Gong W (2021) Embracing self-powered wireless wearables for smart healthcare. In: Proceedings of IEEE PerCom
46. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In: Proceedings of ACM SIGCOMM
47. Yuan L, Gong W (2022) Subscatter: sub-symbol wifi backscatter for high throughput. In: Proceedings of IEEE International Conference on Network Protocols (ICNP)

Part II
Backscatter Communication with Ambient Excitations

Part II discusses in detail how to make use of ambient Wi-Fi signals to provide high-throughput backscatter communications with Wi-Fi 1 (Chap. 5), Wi-Fi 2-3 (Chap. 4), Wi-Fi 4 (Chap. 3), Wi-Fi 5-6 (Chap. 6) standards.

Chapter 3
Spatial Stream Backscatter with Multiplexing Wi-Fi

Abstract This chapter introduces MOXcatter, which is a spatial stream backscatter system that operates on standard multiplexing Wi-Fi signals while preserving ongoing Wi-Fi transmission. The utilization of backscatter Wi-Fi technology provides an innovative, cost-effective, and energy-efficient solution for enabling communication between sensor tags and existing Wi-Fi devices. However, existing Wi-Fi-based backscatter systems have not fully explored the advanced features of the latest Wi-Fi standards, specifically spatial multiplexing, which is a critical component of 802.11n and later versions. MOXcatter enables the backscatter tag to encode the sensing data onto spatial multiplexing Wi-Fi packets, which can be decoded by standard Wi-Fi devices, allowing for simultaneous decoding of both the sensing data and original packets. We demonstrate the practical application of MOXcatter using a sensing system and also discuss the potential enhancements of this design. The prototype of MOXcatter is implemented using FPGAs and standard Wi-Fi devices. The performance evaluation shows that this design achieves a maximum transmission rate of 50 kbps for single-stream Wi-Fi and 1 kbps for double-stream Wi-Fi.

3.1 Introduction

As one of the most popular indoor wireless technologies, 802.11 Wi-Fi has gained popularity for applications of the Internet of Things (IoT). For instance, common smart home products, such as Google Home, use Wi-Fi to deliver service data directly from the cloud and integrate with environmental sensors or controllers, such as thermometers, cameras, and smoke detectors. However, the energy consumption of Wi-Fi is always an issue. Typical Wi-Fi transceivers consume 80 mW of power to transmit 75 data bytes every second. This is 40 times more than Bluetooth [1].

A large part of the power in Wi-Fi and many other active wireless protocols is used to transmit signals. The emergence of backscatter communication has recently altered this landscape [2]. In a traditional backscatter system, a reader generates excitation signals while a backscatter tag modulates and reflects the excitation signal using programmable logic or on-board circuits to control the

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_3

matching impedance of the antennas. Then, the reader decodes the tag data from the reflected signal. This approach is energy-efficient because the tag data is embedded on reflected signals, and the tag can also harvest the energy from ambient radios to power its computation and transmission units without the need for a battery. Backscatter communication has been studied extensively, particularly in the field of Radio Frequency Identification (RFID), which is now widely available at a low cost. Recent research has suggested that backscatter tags can also reflect a range of wireless signals beyond RFID, such as cellular, wireless TV, and Wi-Fi signals, providing a new cost-effective and energy-efficient option for wireless communication [3–11].

The growing interest in using Wi-Fi backscatter for IoT devices may not require the full set of Wi-Fi features. Passive Wi-Fi [12] expands the capabilities of backscatter systems to work with readily available Wi-Fi devices, but it necessitates an extra device to generate excitation signals. Since 2009, all mainstream Wi-Fi protocols, such as 802.11n/ac/ad, have included Multiple Input Multiple Output (MIMO) as a standard feature. For the excitation signals, it is necessary to take into account multiplexing MIMO signals, which are widely used in standard Wi-Fi radios. A Wi-Fi Access Point (AP) can dynamically switch the single-stream and multi-stream modes according to the channel quality [13, 14]. However, some advanced functionalities such as spatial multiplexing have not been explored yet. While HitchHike [15], Inter-Technology Backscatter [4], and FreeRider [16] are all compliant with commodity Wi-Fi, they all work with single-stream signals. Wi-Fi Backscatter [3] and FSBackscatter [5] utilize the Channel State Information (CSI) or Received Signal Strength Indicator (RSSI) instead of spatial streams to transmit tag data.

In this chapter, we introduce MOXcatter, which is a spatial stream backscatter system that uses commodity multiplexing Wi-Fi to exploit the full capabilities of the advanced Wi-Fi standards. MOXcatter can use ambient spatial streams to encode tag data that can be obtained from commodity MIMO Wi-Fi devices. Figure 3.1 illustrates the basic process where spatial multiplexing Wi-Fi is used

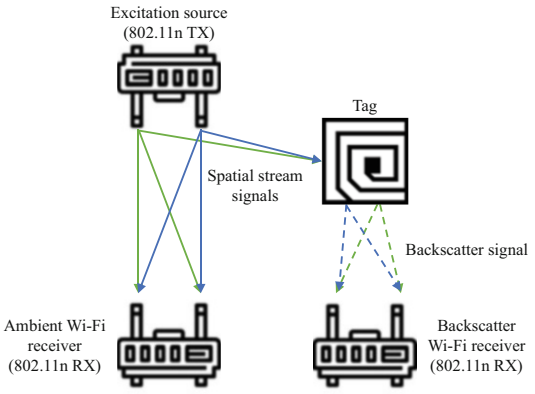


Fig. 3.1 MOXcatter achieves backscatter communication using commodity MIMO Wi-Fi

as the excitation source and the tag employs spatial stream Wi-Fi to carry the tag data. A backscatter Wi-Fi receiver, another standard Wi-Fi device, then decodes the tag data by comparing the received backscatter data with the original data received from the ambient Wi-Fi receiver.

In order to design a backscatter system that works with MIMO Wi-Fi, we face a series of challenges:

- In single-stream signals, each Orthogonal Frequency-Division Multiplexing (OFDM) symbol consists of consecutive bits from the original data stream. However, in multi-stream signals, due to stream parsing, the bits included in a symbol are not consecutive. Therefore, the modulation of a marker bit on separate OFDM symbols cannot be demodulated.
- To avoid a significant increase in bit error rate, tag modulation must be applied to specific data fields in ambient Wi-Fi packets, making synchronization for the tag and the ambient spatial stream signals necessary.
- Furthermore, a tag must be able to work seamlessly with different excitation signals. One possible solution is to include several modulation modes in a tag for various excitation signals, but the switching between them should be automated.

We integrate the following novel designs into MOXcatter to address the above issues:

- We create a modulation rule for our MOXcatter tag to carry tag data by changing the OFDM symbol phase. A 0° or 180° phase change is used to indicate a '0' or '1' bit. This phase change is applied to separate symbols to allow single-stream packets with several tag bits, and to the entire data fields to allow multi-stream packets with one tag bit.
- We also design a decoding scheme that compares the backscattered data with the original data. The process finds every all-0 (or all-1) series in the XOR result of the backscattered data and the original data. The all-0 and all-1 series correspond to the 0° and 180° phase change introduced by the tag, respectively.
- We design the patterns of control signals, which can be received using the Wi-Fi signal detector within the backscatter tag. The appropriate backscatter circuits for various excitation signals are automatically selected in our design.

The prototype of our MOXcatter tag, which includes a Field Programmable Gate Array (FPGA) and Radio Frequency (RF) front-end circuits are shown in Fig. 3.2.

In this chapter, we investigate the strategies to improve the throughput, especially in the case of multi-stream signals. Additionally, we demonstrate the versatility of our design by presenting a sensor system that solely relies on MOXcatter tags and off-the-shelf Wi-Fi devices.

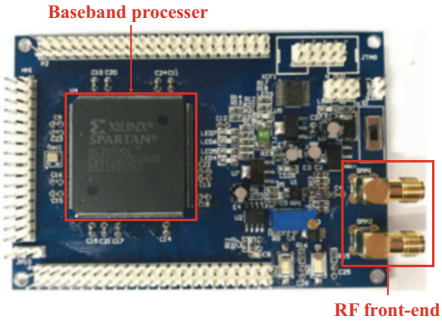


Fig. 3.2 MOXcatter tag prototype

3.2 Related Work

Backscatter communication has gained popularity due to its cost-effectiveness and energy efficiency [3–12, 15, 17–32]. Typically, an external reader generates the excitation signal, decodes the backscatter signal, and retrieves the tag data in the backscatter system. Some recent research has shown that rather than using dedicated readers or customized signals, ambient wireless signals such as cellular, Bluetooth, ZigBee, and Wi-Fi can also be utilized for backscatter excitation. Of these signals, Wi-Fi is particularly noteworthy since it is considered the most prevalent wireless communication technology for indoor use.

In recent years, researchers have made significant progress in designing backscatter systems that are compatible with Wi-Fi technology. Wi-Fi Backscatter [3], BackFi [17], and Passive Wi-Fi [12] are pioneering studies that have contributed to this progress. Wi-Fi Backscatter is the first system to use Wi-Fi devices to connect backscatter tags to the Internet. The system modulates the tag information by reflecting and absorbing original Wi-Fi packets. The change in CSI/RSSI information in the backscattered packet enables the decoding of the tag data. BackFi, on the other hand, designs an IoT sensor that uses backscattered Wi-Fi signals. Customized radio circuits on a Wi-Fi AP are required to decode the backscattered signals. Passive Wi-Fi can achieve 10,000 times lower power consumption than standard Wi-Fi communication. Recent studies also addressed compatibility and deployment problems. For example, Inter-Technology Backscatter [4] change wireless transmission from one protocol to another. It backscatters Bluetooth radios to generate Wi-Fi radios, enabling communication between commodity Wi-Fi and Bluetooth radios. FS-Backscatter [5] uses frequency shift to separate the backscatter signals from the excitation source to eliminate self-interference and decode tag data with high quality. HitchHike [15] embeds tag bits in 802.11b packets, enabling backscatter communications using only commodity Wi-Fi devices. FreeRider [16] uses codeword translation [15] that works with many commodity wireless signals, including single-stream OFDM Wi-Fi, ZigBee, and Bluetooth.

MIMO is widely used in Wi-Fi devices based on 802.11n and beyond, and the evolution of Wi-Fi technology is fast. However, MIMO has not been thoroughly

explored in Wi-Fi-based backscatter communication systems. Previous work has mostly been limited in that it has examined CSI or RSSI rather than spatial streams [3, 5], only supported single-stream signals [4, 15, 16], or relied on dedicated but incompatible circuits [17]. Zhao et al. [33] is the first to demonstrate that backscatter communication is possible with spatial streams in 802.11n and above. It is capable of embedding tag data in the data fields of spatial stream Wi-Fi and decoding the information using a MIMO Wi-Fi AP without any hardware changes. It is also backward compatible and can be used to backscatter 802.11b/g signals.

3.3 Codeword Translation for Spatial Stream Wi-Fi

In advanced Wi-Fi standards, including 802.11n/ac/ax, the MIMO-OFDM radio, which uses spatial multiplexing, becomes the primary PHY air interface. Since our MOXcatter design explores these operations, we provide a brief introduction to them in Sect. 3.3.1. In Sect. 3.3.2, we will demonstrate how phase changes can be used to modulate tag data and create a backscattered packet that is compatible with Wi-Fi protocols.

3.3.1 Spatial Stream Wi-Fi Primer

Figure 3.3 shows a typical spatial stream transmission process that involves the following transform operations [34–37].

Scrambling To prevent negative effects on symbol synchronization when all-0 or all-1 long sequences occur frequently, it is common practice to introduce scrambling in digital communications. The purpose of scrambling is to interrupt these long sequences of repeated bits of data and transform the statistics of the transmitted message into an approximation of white noise. Wi-Fi transmitters create a fixed-length bit sequence for the data field using a frame-synchronous scrambler. The original data is then combined into a stream and processed through an XOR gate, which can be represented as

$$ScrambledData = OriginalData \oplus ScramblerOut \tag{3.1}$$

Convolutional Encoding Convolutional encoding generates coded bits based on both the current input bit and the previous input bits. Due to its low delay, convolutional encoding is well-suited for serial data transmission. The coding rate R is determined by the ratio of the number of output bits n to the number of input bits k. The different modulation coding schemes (MCS) and coding rates of 802.11 Wi-Fi correspond to various speeds, such as 6.5 Mbps Binary Phase Shift Keying (BPSK)

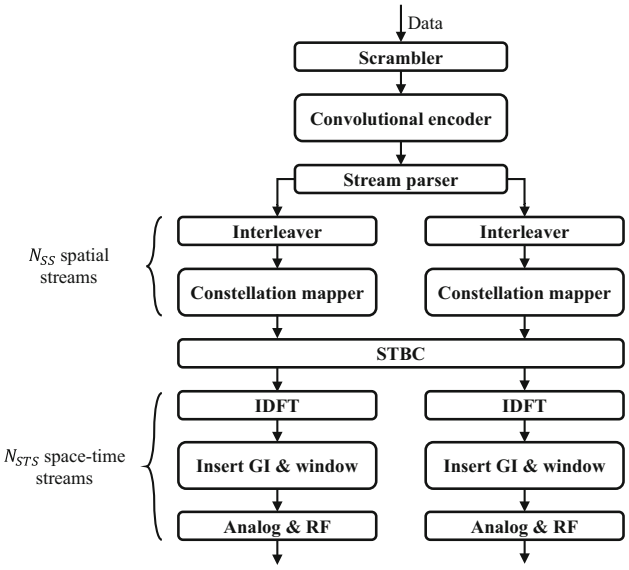


Fig. 3.3 MIMO Wi-Fi transmitter

with $R = \frac{1}{2}$, 19.5 Mbps Quadrature Phase Shift Keying (QPSK) with $R = \frac{3}{4}$, and 65 Mbps 64 Quadrature Amplitude Modulation (QAM) with $R = \frac{5}{6}$.

Stream Parsing A stream parser is used to split the encoded data into blocks of bits of length s, which are then sent to different interleavers. s can vary depending on the specific modulation and standard used. For instance, in 802.11n, for a 6.5 Mbps signal using BPSK modulation, the block size is $s = 1$. The data that is sent to an interleaver is referred to as a spatial stream. The stream parser allocates successive blocks of data bits to different spatial streams in a round-robin fashion. In our work, we use the spatial stream data to carry information.

Interleaving Interleaving rearranges data in a non-continuous fashion to combat serial or burst bit errors. This technique overcomes bit errors that typically occur in some of the serial bits by rearranging data in a non-continuous manner. By doing so, a long sequence of bit errors is transformed into shorter sequences. This enables forward error correction to correct the shorter strings of error bits.

Constellation Mapping The modulation techniques for OFDM subcarriers comprise BPSK, QPSK, 16-QAM, 64-QAM, and 256-QAM. To map coded data bits onto the constellation, each subcarrier uses the corresponding modulation method to generate a complex point.

STBC Space-time block coding (STBC) spreads constellation points from N_{SS} spatial streams into N_{STS} space-time streams. One spatial stream is expanded into two space-time streams with orthogonality. STBC is optional and is used to provide

robust transmission. If the transmission channel is unreliable for high throughput transmission due to its poor quality (e.g., high propagation delay, strong channel attenuation, or massive carrier frequency offset), the MIMO transmitter can use STBC to reduce errors by increasing redundancy.

Inverse Discrete Fourier Transform (IDFT) IDFT converts a block of constellation points into time domain signals. After the IDFT, the OFDM symbols are then ready for the multiplexing of the carrier wave for transmission.

3.3.2 Tag Codebook Design for Advanced Wi-Fi

Once the spatial stream signal is identified, the tag information can be conveyed through phase modulation in the OFDM symbols. Let $y_r^{(n)}$ denote the I/Q data on the subcarrier r of the nth symbol, where m represents the total number of coded data in a symbol. The coded data is a sequence of complex numbers represented as $Y_n = \{y_1^{(n)}, y_2^{(n)}, \ldots, y_m^{(n)}\}$. The vector $\mathbf{Y} = [Y_1, Y_2, \ldots, Y_l]'$ represents the transmitted symbols.

Tag modulation technique in MOXcatter employs a codebook to determine the phase shifts applied to each subcarrier. We use a vector $\Theta = [\theta_1, \theta_2, \ldots, \theta_l]$ to represent tag modulation. Subcarrier modulation using BPSK can be modulated with $\theta_i \in \{-1, 1\}, i \in \{1, \ldots, l\}$, while MCS from QPSK to 64-QAM can be modulated with $\theta_i \in \{e^{-j\frac{\pi}{2}}, e^{j\frac{\pi}{2}}, -1, 1\}, i \in \{1, \ldots, l\}$. The modulated OFDM symbols can be expressed by multiplying the original subcarriers $\mathbf{Y}$ with the tag modulation vector Θ:

$$\mathbf{Y}^{tag} = \Theta\mathbf{Y}. \tag{3.2}$$

Now we will explain why backscattered packets remain valid OFDM Wi-Fi packets and why our tag modulation and demodulation are not affected by operations such as scrambling, convolutional coding, interleaving, and IDFT.

Consider single stream 6.5 Mbps 802.11n signals. The Wi-Fi transmitter uses the complex number of the 52 data subcarriers Y_n and the values of the 4 pilot subcarriers to create a new sequence $X_n = Inst(Y_n)$ which is used as input to the IDFT to generate an OFDM symbol. IDFT is formulated as follows:

$$x_n(t) = IDFT\,[X_n(k)] = \frac{1}{K}\sum_{k=0}^{K-1} X_n(k)e^{j\frac{2\pi}{K}kt}. \tag{3.3}$$

Here, $t = 0, 1, \ldots, K$ is the index of subcarriers. $x_n(t)$ is the discrete-time signal of symbol n and will be used for transmission after multiplying the carrier. The pilot values are for synchronization only and have no effect on demodulation at the receiver. Thus, the above transform is linear. As the tag modulation operates on the

nth OFDM symbol, it satisfies the equation:

$$\theta_n \cdot IDFT\left[Inst(Y_n)\right] = IDFT\left[Inst(\theta_n \cdot Y_n)\right]. \tag{3.4}$$

The backscattered signal is processed using Eq. 3.4 on the backscattered channel, which has a constant frequency offset from the original excitation channel. However, if the tag modulates the OFDM symbol phase, the I/Q data is altered. It is crucial to ensure that the modified data remains compatible with the subcarrier demodulation process at the receiver.

Let $C_n = \{c_1^{(n)}, \ldots, c_q^{(n)}\}$ represent the original data of the nth symbol with q bits for each symbol for a given MCS. The scrambled data sequence is denoted as $D_n = \{d_1^{(n)}, \ldots, d_q^{(n)}\}$ and the data sequence generated after scrambling is $S_n = \{s_1^{(n)}, \ldots, s_q^{(n)}\}$. We can express D_n as:

$$D_n = S_n \oplus_n C, \tag{3.5}$$

according to Eq. 3.1. Since the convolutional coding, interleaving, and IDFT involved in the signal processing are linear operations, we can define a linear transform $V(\cdot)$ that maps the original data sequence C_n to a data sequence after tag modulation C_n'. Thus, we have $\theta_n \cdot x_n = V(S_n \oplus C_n')$.

The Wi-Fi receiver demodulate data as follows:

$$V^{-1}\left(\theta_n \cdot x_n\right) \oplus S_n = S_n \oplus C_n' \oplus S_n = C_n'. \tag{3.6}$$

According to the illustration in Fig. 3.4 as well as the tag codebook in Table 3.1, C_n and C_n' share the same codebook. In QPSK, 16-QAM, and 64-QAM, the four phases from 0° to 270° preserve the backscattered signals within the same constellation, hence carrying two tag bits.

In a multi-stream 802.11n system, the phase change tag modulation is not a linear transformation of the encoded data due to stream parsing and STBC. After stream parsing, an OFDM symbol on a spatial stream may contain non-consecutive bits

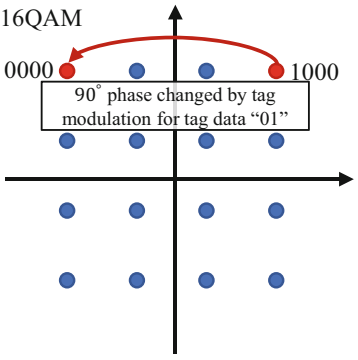


Fig. 3.4 An example of why the backscattered subcarrier data is still in the QAM constellation and can therefore still can be demodulated by a commodity off-the-shelf Wi-Fi device

Table 3.1 Tag codebook design for spatial stream Wi-Fi

Subcarrier modulation	Phase change	Tag data
BPSK	0°	0
	180°	1
QPSK, 16-QAM, 64-QAM	0°	00
	90°	01
	180°	10
	270°	11

in comparison to the original data bit stream. Moreover, if the STBC is enabled, the multi-stream signals thus have orthogonality. Such orthogonality may be ruined in our tag modulation, resulting in data demodulation at the receiver fails. Since the above two operations in multi-stream Wi-Fi cause Eq. 3.6 to no longer hold in each spatial stream, the phase change cannot be decoded in the single-stream design. However, we can still embed one tag bit onto each multi-stream packet using phase shifts of 0° or 180° on the entire PPDU fields, rather than on individual OFDM symbols. The backscattered multi-stream PPDU fields remain intact if the tag applies 0° phase changes. However, it changes if a 180° phase change is used.

3.4 MOXcatter Design

Our MOXcatter's architectural design is depicted in Fig. 3.5. This section details the design of some critical modules such as signal detection, tag modulation, information decoding, and control signaling.

3.4.1 Wi-Fi Signal Detector

The circuit board of our tag design has a signal detector located between the antenna and the FPGA. This front-end analog circuitry converts the incoming Wi-Fi power signal into a binary high/low voltage signal for the digital circuitry of the FPGA. A high voltage signal is output if the detector detects a Wi-Fi signal, while a low voltage is output otherwise. Figure 3.6 shows that the design of the detector consists of two parts: a multi-stage demodulating logarithmic amplifier and a voltage comparator. Each amplifier stage is connected to a diode detector and the multi-stage outputs are added together and sent to a low pass filter (made up of R_1 and C_1). The output V_{RF} is proportionate to the amplitude of the received signal. If the received Wi-Fi signal strength is dBm_{RF}, then V_{RF} can be formulated as follows:

$$V_{RF} = K \cdot dBm_{RF}, \tag{3.7}$$

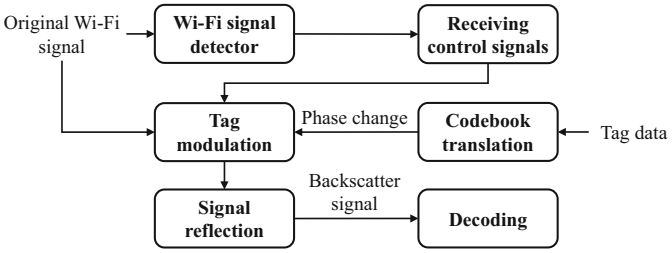


Fig. 3.5 Overview of system design

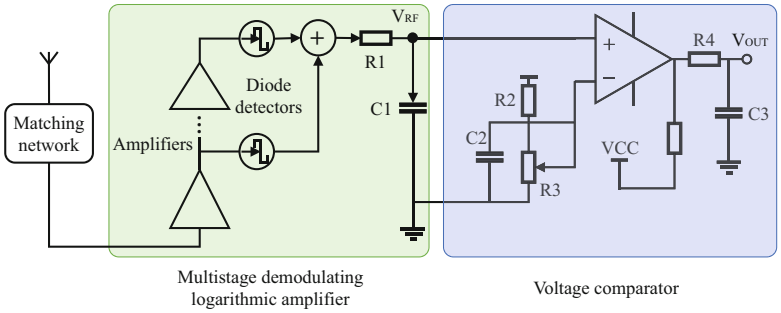


Fig. 3.6 Wi-Fi signal detector circuit design

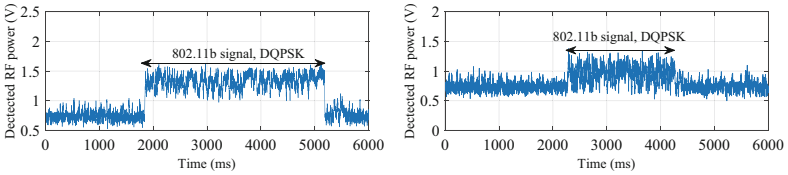


Fig. 3.7 Signal durations using different modulation (2000 packets with packet 556 bytes packet size)

where K is a scaling factor that remains constant within the range of operation bounded by the intersection and saturation points.

The voltage comparator circuit is used for noise elimination. We noticed that the Wi-Fi signal strength is typically considerably higher than the noise, for example, 30 dB. Therefore, a threshold voltage can be used to detect the Wi-Fi signal. Figure 3.6 shows that we use a sliding rheostat R_3 to adjust the threshold V_{ref}. When the input of the comparator V_{RF} is greater than V_{ref}, VOUT is '1', otherwise, it is '0'.

Figure 3.7 shows the voltage V_{RF} traces for two packets with different modulations captured during Wi-Fi transmission using a commodity Wi-Fi device. Each experiment involved sending 2000 packets of 556 Bytes, using two different modulation techniques: 802.11b Differential QPSK (DQPSK) and 802.11n 2×2 MIMO BPSK. The detector identifies the beginning, ending, and duration of the

Wi-Fi packet. The positive edge at the start and the negative edge at the end of the signal can be used as a trigger signal for the FPGA circuits.

3.4.2 Tag Modulation

As per the analysis in Sect. 3.3.2, changing the phase of an OFDM symbol using MOXcatter tag's codebook in Table 3.1 can enable decoding of the backscattered signal by commodity Wi-Fi devices. The MOXcatter tag uses phase modulation, which is achieved by multiplying the ambient excitation signal with a phase-varying square-wave signal. The phase of this square wave changes as the tag data changes. Figure 3.8 illustrates that the backscatter tag will not modify the phase of the preamble in the PHY Layer Convergence Procedure (PLCP) and the MAC header in the PLCP Protocol Data Unit (PPDU) to undertake that backscatter packets can be received. OFDM symbol phase changes based on the codebook and the modulated tag data.

To transmit the backscattered 802.11n packets, our backscatter tag uses frequency shift. The tag uses an RF switch to perform multiplication. The switch is controlled by a phase-varying square-wave on/off signal at frequency f_t. The carrier frequency of the original signal is f_c. Let $\omega_t = 2\pi f_t, \omega_c = 2\pi f_c$, and $\alpha_{base}(t)$ be the baseband Wi-Fi signal. Then we have the square wave $M_{tag}(t) = \frac{4}{\pi}\sum_{n=1}^{\infty}\frac{\sin((2n-1)\omega_t t)}{2n-1}$, and the backscattered signal, $\beta(t)$, can be written as

$$\beta(t) = \alpha_{base}(t)e^{j\omega_c t}M_{tag}(t). \tag{3.8}$$

Let $F_{base}(\omega)$ denote the Fourier transform of $\alpha_{base}(t)$, and $F(\omega)$ represent the Fourier transform of $\beta(t)$. Thus, we have

$$\begin{aligned} F(\omega) = \sum_{n=1}^{\infty}\frac{2j}{\pi(2n-1)}(&F_{base}(\omega-\omega_c+(2n-1)\omega_t) \\ &- F_{base}(\omega-\omega_c-(2n-1)\omega_t). \end{aligned} \tag{3.9}$$

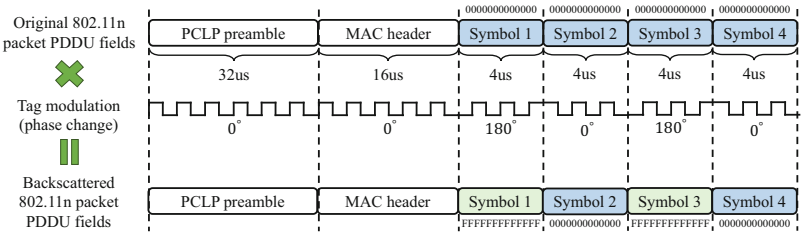


Fig. 3.8 Tag modulation: the tag multiplies the original signal with the tag modulation signal. The tag modulation signal applies a phase change to a square wave to represent tag information

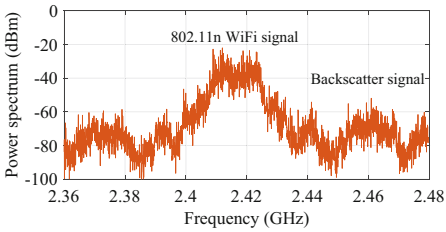


Fig. 3.9 Spectrum of the original 802.11n Wi-Fi signal and the backscatter signal. The backscatter signal is shifted from 2.417 to 2.467 GHz

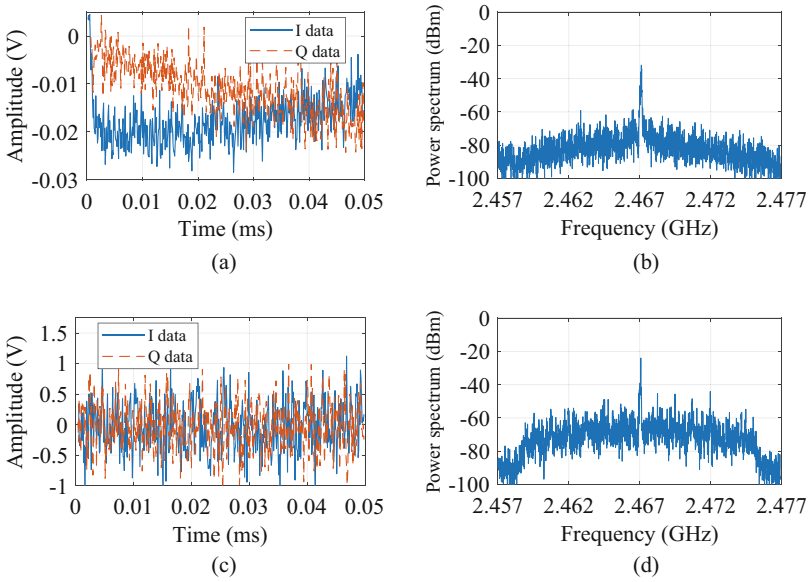


Fig. 3.10 Backscattered Wi-Fi signal obtained at the center frequency of 2.467 GHz. We transmit the original Wi-Fi signal at the center frequency of 2.417 GHz and the tag backscatter it using 50 MHz frequency shift. (**a**) Baseline in time domain. (**b**) Baseline at 2.467 GHz. (**c**) Backscattered signal in time domain. (**c**) Backscattered signal at 2.467 GHz

The received backscattered signal is detected in the frequency $\frac{2}{\pi}|F_{base}(\omega - \omega_c - \omega_t)|$. Figure 3.9 shows an illustration of the spectrum. Additionally, Fig. 3.10 depicts the captured time and frequency domain backscattered signals and compares them to the baseline noise signal.

3.4.3 Tag Information Decoding

Commodity Wi-Fi devices with multiple antennas, like an 802.11n Network Interface Card (NIC), are used for receiving and decoding the backscattered signal.

The original and the backscattered Wi-Fi packets are captured at different center frequencies with a fixed difference. These two signals are combined and used for tag data decoding in two steps.

We employ the decoder proposed by Zhang et al. [15] in the first step. The original packets are received at the carrier center frequency of 2.417 GHz, while the backscattered packets are received at 2.467 GHz. The original data is denoted as $\mathbf{Q} = \{Q_1, \ldots, Q_n\}$, where Q_i contains the data bits of the ith symbol. The backscattered 802.11n data is denoted as $\mathbf{B} = \{B_1, \ldots, B_n\}$, where B_i denotes the bits of the ith symbol. With $\mathbf{Q}$ and $\mathbf{B}$ we do XOR operations:

$$\Gamma_i = Q_i \oplus B_i, \tag{3.10}$$

where $\Gamma_i, i \in 1 \ldots n$ is the processed raw data of the ith symbol. The length of Γ_i varies depending on the MCS. For example, for 802.11g signal, BPSK MCS with rate $\frac{1}{2}$, $|\Gamma_i| = 24$. For 802.11n, BPSK MCS with rate $\frac{1}{2}$, $|\Gamma_i = 26|$ for single-stream signal, and $|\Gamma_i = 52|$ for double-stream signal. However, the codeword translation proposed in [15] can only decode the tag data at the bit level. It is also limited to 802.11b signals. Therefore, our system requires an additional step to decode the tag data at the symbol level.

Our second step is to find and decode sequences of fixed length $|\Gamma_i|$. For instance, in BPSK subcarrier modulation, the sequence can be either all-0 or all-1. We can decide how many symbols to use to carry a tag bit in tag modulation. When we use two symbols to carry a tag bit in BPSK subcarrier modulation, the time-domain signal of these OFDM symbols undergoes a phase shift of 180°. In tag data decoding, we employ a decoding window whose length is the number of symbols for a single tag bit. Based on our observation, burst bit errors appear near the phase change from 0° to 180° or vice versa, i.e., transitioning from a long sequence of all-0 or all-1 bits to a long sequence of all-1 or all-0 bits. This problem can result in decoding failure when we use one symbol for a single tag bit. To address this issue, we can use two symbols for a tag bit in BPSK MCS with a single spatial stream. Doing so ensures that there is always an all-0 or all-1 sequence of length $|\Gamma_i|$ within our decoding window, making our decoding valid. We can denote an all-1 sequence of length $|\Gamma_i|$ for the jth tag bit as Λ_j, and $\Phi_i = \Gamma_i, \Gamma_{i+1}$, where $i = 2j - 1$, and j is a positive integer. We search an all-1 sequence using the following algorithm:

$$\eta* = \underset{\eta \in \{1,\ldots,|\Gamma_i|\}}{\operatorname{argmax}} \left| \sum_{k=0}^{|\Gamma_i|} \Lambda_j[k] \Phi_j[\eta + k] \right|, \tag{3.11}$$

where $\eta*$ denotes the beginning of the valid data sequence. To search for an all-0 sequence in Eq. 3.11, argmax can be changed to argmin.

A decoding example is presented in Fig. 3.11, where a tag sends "101" with a single-stream signal. Decoding tag data using one symbol per bit may fail for BPSK MCS as mentioned above. Decoding the tag data with a window length of $2|\Gamma_i|$

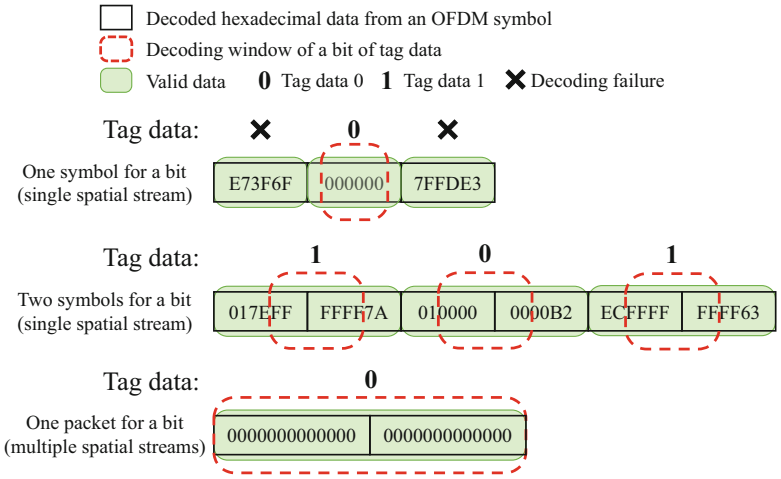


Fig. 3.11 Tag data decoding. We use a decoding window and search for fixed-length all-1 or all-0 sequences

enables successful decoding. The valid data for decoding consists of only the first all-0 (or all-1) sequence of length $|\Gamma_i|$ in our searching window. Our analysis in Sect. 3.3.2 indicates that only one tag bit can be embedded in each double-stream packet. As shown in Fig. 3.11, decoding an all-zero sequence from the data fields of a double-stream backscattered packet indicates tag data 0, otherwise, tag data is 1.

3.4.4 Control Signals

The Wi-Fi signal detector output can measure Wi-Fi packet durations, which can be used to design the patterns of the control signals. This feature enables our backscatter tag to handle different excitation signals. We use various 802.11 PHY to generate control signals, each control signal has four consecutive Wi-Fi packets of 2024 bytes. Figure 3.12 shows the patterns of different control signals obtained from the signal detector. We find that the packet duration is accurately measured by the digital circuit of FPGA. For instance, one packet transmitting 2024 Bytes data takes 16540 μs at 1 Mbps 802.11b, 2720 μs at 6 Mbps 802.11g, and 671 μs at 13 Mbps double-stream 802.11n. Such information, in particular the average duration of Wi-Fi packets in the received control signal, can be used by the tag as a trigger condition for corresponding backscatter modes. The number of recognizable excitation signal types can be increased, subject to the processing speed and resources of the FPGA.

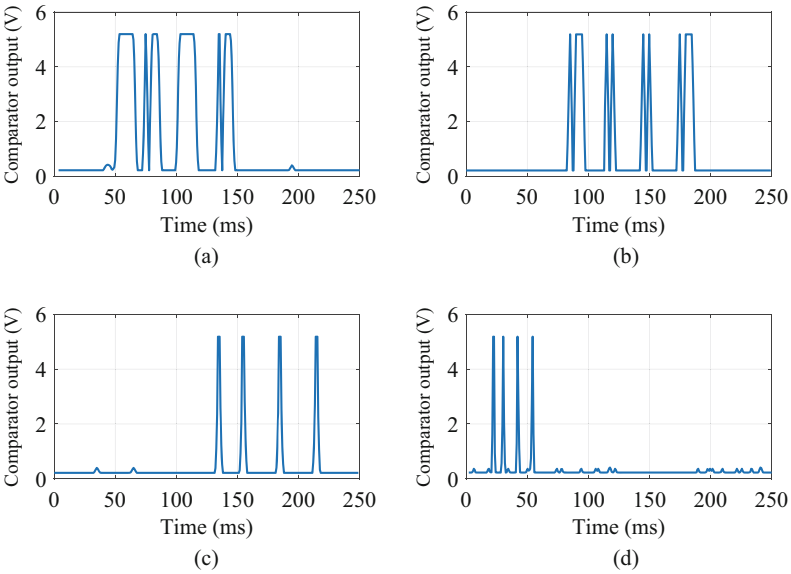


Fig. 3.12 Response of the signal detector (in Fig. 3.6) to four consecutive Wi-Fi packets using different PHY types (packet size 2024 bytes). Different PHY types have different output patterns. (**a**) 802.11b DBPSK. (**b**) 802.11b DQPSK. (**c**) 802.11g at 6 Mbps. (**d**) 802.11n 2x2 MIMO at 13 Mbps

3.4.5 Symbol-Level Modulation in Multi-Stream Wi-Fi

While packet-level tag modulation works well in multi-stream signals, it significantly reduces the transmission efficiency compared to symbol-level tag modulation in single-stream signals. According to the analysis in Sect. 3.3.2, the barriers that prevent us from implementing symbol-level modulation are the non-consecutive problem and the orthogonality problem. If we solve these problems to allow tag modulation in multi-stream signals at the symbol level, the tag can modulate more bits in a packet, thus increasing the throughput. We now present some possible solutions to these problems.

Non-consecutive Problem Due to the round-robin allocation of bits to spatial streams by stream parsing, each OFDM symbol on a single spatial stream contains non-consecutive coded bits. However, encoded bits in OFDM symbols with the same index in all spatial streams are consecutive segments in the original encoded data sequence. The Wi-Fi receiver will decode the spatial streams to recover the original encoded data sequence after deinterleaving. Therefore, we use the symbols with the same index in different spatial streams to carry phase change and embed tag data. The tag can also synchronize and modulate with them as these symbols are transmitted simultaneously.

Orthogonality Problem STBC brings orthogonality to multi-stream signals to achieve full diversity gain. As the tag applies a phase change to multi-stream signals, it can destroy the orthogonal property, making the standard Wi-Fi receiver unable to recover the encoded data. The STBC processes spatial streams in blocks of two consecutive OFDM symbols. A coding matrix can be used to describe the stream parser using transmission diversity:

$$\mathbf{X} = \begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix} \tag{3.12}$$

Where x_1, x_2 are two modulated symbols in a block in a spatial stream and $(\cdot)^*$ is the conjugate transpose. Each row of $\mathbf{X}$ is transmitted in a space-time stream. STBC fulfills full diversity since the following equation holds:

$$\mathbf{X}^H\mathbf{X} = \lambda\mathbf{I} \tag{3.13}$$

where $\lambda \in \mathbb{R}$, $\mathbf{I}$ represents the identity matrix and $(\cdot)^H$ denotes the conjugate transpose. To solve this problem, we ensure that orthogonality holds after tag modulation by performing the phase change on a whole block of space-time. Let $\mathbf{X_B} = \theta\mathbf{X}$ represent the block-level tag modulation, then we have:

$$\mathbf{X_B}^H\mathbf{X_B} = \theta\theta^*\mathbf{X}^H\mathbf{X} = \lambda'\mathbf{I} \tag{3.14}$$

where $\lambda' \in \mathbb{R}$. It reveals that the orthogonality holds.

3.5 Performance Evaluation

3.5.1 Implementation and Setup

Detector Circuits A Wi-Fi signal detector was developed by integrating key periphery circuits with the main integrated circuits. According to the design in Fig. 3.6, the multi-stage demodulating logarithmic amplifier uses an AD8313 connected to a matching network and a low pass filter. The voltage comparator uses a TLV3501, a threshold voltage matching circuit, and a low-pass filter. Our implementation sets the threshold at 1.25 V by adjusting the sliding rheostat.

FPGA Digital Circuits To host the tag modulation module and control signal receiving module, we use the XILINX Spartan XC3S500E-4PQ208 FPGA. When the detector outputs a positive edge, it triggers the Digital Clock Manager (DCM) module of the FPGA to generate a square wave for tag modulation. The module outputs four square waves with phase changes from 0° to 270°. The tag data outputs connect to two selection pins of a 4 to 1 multiplexer, and the output of

the multiplexer is selected based on the codebook in Table 3.1. This output controls an ADG902 RF switch.

Packet Transmission and Reception We use two off-the-shelf PCs, each equipped with a Qualcomm Atheros AR938x NIC. Both PCs act as excitation signal generators and backscatter signal receivers. To simplify the process, we use CommView for Wi-Fi [38], which is an 802.11a/b/g/n/ac wireless network analyzing tool. The transmitter generates the excitation signals using this tool, while the receiver retrieves the backscattered data through it. We apply the searching algorithm outlined in Sect. 3.4.3 to decode the tag data from the backscattered data.

Experiment Setup We carry out our experiments in an indoor area with a size of 33×15 m. The receiver begins at a distance of 2 m from the tag and moves along the corridor. Every experiment involves the measurement of the Received Signal Strength Indicator (RSSI), Bit Error Rate (BER), and throughput. The MOXcatter tag is powered externally with 5 V during the measurements, and the distance between the backscatter tag and the transmitter is 0.3 m.

3.5.2 Evaluation

This section focuses on evaluating the performance of MOXcatter in both line-of-sight (LoS) and non-line-of-sight (NLoS) scenarios. Firstly, we measure the strength of the backscattered signal across different communication distances and physical layer configurations. Following that, we analyze the bit error rate (BER) and throughput of the tag data.

3.5.2.1 Backscatter Signal Strength

We conducted an experiment to measure the RSSI of the backscattered signal. To generate the Wi-Fi excitation signals, we used four different physical layer specifications: 802.11b QPSK at 2 Mbps, 802.11g OFDM BPSK MCS at 6 Mbps, 802.11n Single-Stream (SS) BPSK MCS at 6.5 Mbps, and 802.11n Double-Stream (DS) BPSK MCS at 13 Mbps. The excitation signal was produced at Channel 2 (2.417 GHz), and the backscattered signal was shifted to Channel 12 (2.467 GHz).

Figure 3.13 displays the backscattered RSSI at various tag-to-RX distances in the LoS scenario. The RSSI value generally decreases with an increase in backscatter communication distance for all three cases, although there are some fluctuations. At a distance of 14 m, the RSSI values for all three cases drop below -80 dBm.

Figure 3.14 presents the Cumulative Distribution Function (CDF) of the RSSI in our NLoS experiments. The results indicate that at a distance of 2 m, the backscattered 802.11n signals exhibit higher RSSI than 802.11g.

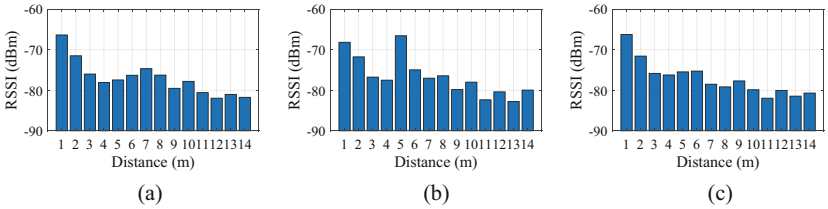
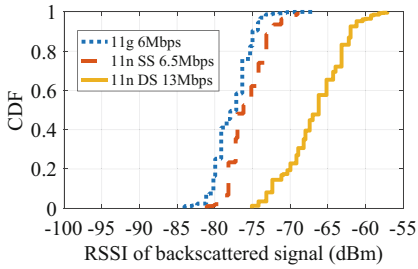


Fig. 3.13 Backscatter RSSI varies with tag-to-RX distance in LoS experiments. (**a**) 802.11g at 6 Mbps. (**b**) 802.11n SS at 6.5 Mbps. (**c**) 802.11n DS at 13 Mbps

Fig. 3.14 Backscattered RSSI in NLoS experiments



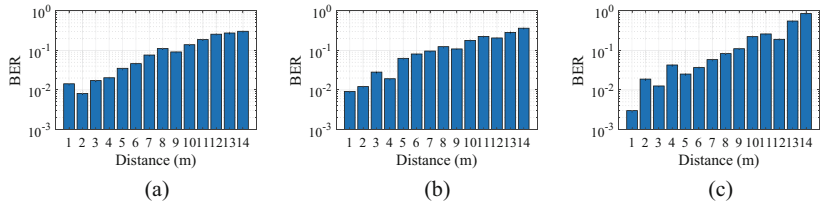


Fig. 3.15 Tag data BER varies with tag-to-RX distance in LoS experiments. (**a**) 802.11g at 6 Mbps. (**b**) 802.11n SS at 6.5 Mbps. (**c**) 802.11n DS at 13 Mbps

3.5.2.2 Bit Error Rate

Next, we conducted experiments to measure the BER in our backscatter experiments. In Fig. 3.15, we plot the BER of the decoded tag data against the tag-to-RX distance in the LoS experiments. When the tag-to-RX distance is less than 3 m, the BER remains below 0.06. As expected, the BER increases with distance, and it becomes very high when the distance exceeds 14 m, especially for the backscattered 802.11n DS signals.

In Fig. 3.16, we show the BER of tag data in the NLoS experiments. Our results demonstrate that single-stream backscatter communication outperforms the double-stream case, even though the working tag-to-RX distances in both cases are shorter than those in the LoS scenario.

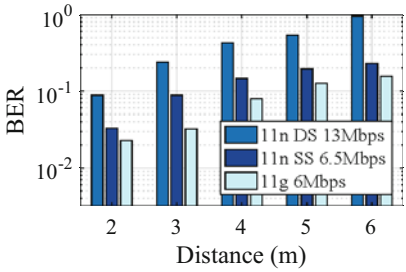


Fig. 3.16 Tag data BER in NLoS experiments

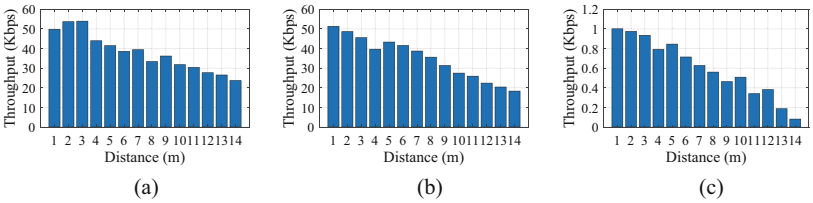


Fig. 3.17 Backscatter throughput varies with tag-to-RX distance in LoS experiments. (**a**) 802.11g at 6 Mbps. (**b**) 802.11n SS at 6.5 Mbps. (**c**) 802.11n DS at 13 Mbps

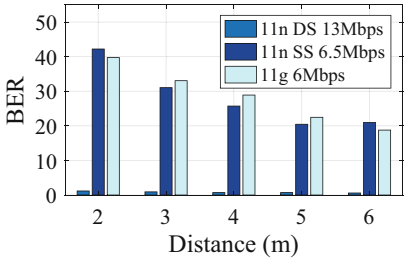


Fig. 3.18 Backscatter throughput in NLoS experiments

3.5.2.3 Throughput

Additionally, we conducted experiments to evaluate the throughput of MOXcatter in LoS and NLoS scenarios.

According to Fig. 3.17, the throughput typically declines for all three cases as distance increases. The backscattered single-stream signals can achieve over 40 kbps when the tag-to-RX distance is less than 6 m. On the other hand, with double-stream signal, the throughput drops to less than 1 kbps since an 802.11n DS packet can only carry one tag bit.

In the NLoS experiments, we found that the single-stream backscattered 802.11n has similar throughput to the 802.11g, where the communication range is still limited to 6 m, as shown in Fig. 3.18.

3.6 Application Case

We believe MOXcatter enables lots of IoT applications with 802.11n Wi-Fi serving as the hub for data exchange. In Sect. 3.5.2, experimental results indicate that our MOXcatter tag can communicate with commodity Wi-Fi receivers with a distance of up to 14 m. The backscatter throughput can reach up to 50 kbps within a range of 0 m to 3 m. This has great potential for indoor sensing systems in smart home designs and other IoT applications such as healthcare systems, smart control systems, and indoor positioning systems.

We implemented a low-power sensor communication system as illustrated in Fig. 3.19. The system consists of a DS18B20 digital thermometer, a prototype of a MOXcatter tag, and a sink node, which is an 802.11n Wi-Fi adapter but also acts as a source of the excitation signal. The thermometer acquires temperature data and sends it as the MOXcatter tag's input, which is later transmitted to the sink node through backscatter communication. The MOXcatter tag's FPGA contains both the DS18B20's and Light-Emitting Diode (LED) display's drive circuit modules.

The DS18B20 drive module can produce a time-varying tag modulation signal by converting 16 bits of parallel temperature data into serial data. The 802.11n SS at 6.5 Mbps transmission is used as the excitation signal, with all data fields set to zero in each packet. The tag encodes temperature data during backscatter by embedding it in the excitation Wi-Fi packets, which the Wi-Fi sink captures and decodes.

Figure 3.20 plots the CDF of the temperature data refresh intervals at the sink node. More than 90% of the intervals are less than 5 ms. Figure 3.21 depicts the instantaneous transmission rate in one second.

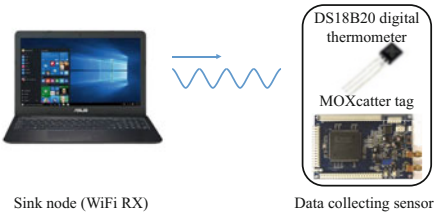


Fig. 3.19 MOXcatter-based data collecting sensor communications

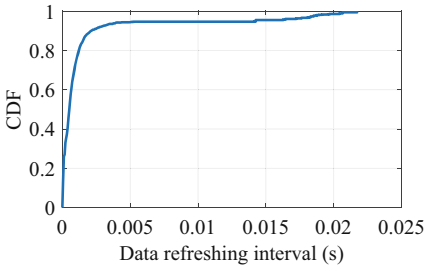


Fig. 3.20 Distribution of temperature data refreshing intervals

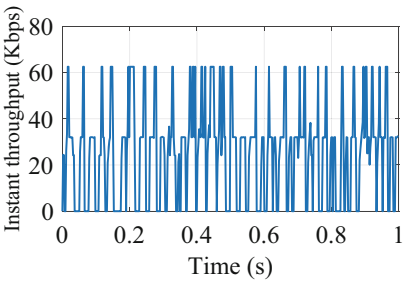


Fig. 3.21 Instantaneous throughput of collecting temperature data

3.7 Discussion

3.7.1 Throughput Enhancement

High-throughput wireless transmission enables various IoT applications, such as real-time Blu-ray video streaming. Advanced Wi-Fi utilizes a high-order MCS, short guard interval, high bandwidth, and spatial multiplexing to enhance its throughput. Consequently, increasing the throughput is naturally expected for backscatter communication based on Wi-Fi. However, our experimental results demonstrate that our MOXcatter achieves a throughput of up to 50 kbps with single-stream signals and up to 1 kbps with double-stream signals in 802.11n, with potential for enhancement.

We notice that the throughput with multi-stream excitation is lower than with single-stream excitation. As we analyzed previously, MOXcatter modulates tag data on a symbol level with single-stream excitation and on a packet level with multi-stream excitation. This results in higher throughput with single-stream excitation than with multi-stream excitation. With symbol-level modulation, a packet can piggyback more tag bits by simply using a long Wi-Fi packet. However, this does not work with packet-level modulation. To make the symbol-level modulation still work for MIMO, we may address the non-consecutive problem and orthogonality problem mentioned in Sect. 3.4.5.

In single-stream signals, our MOXcatter performs phase changes on two consecutive symbols. While such redundancy reduces the transmission error rate and provides reliable transmission, it reduces transmission throughput. If we can design a better tag information decoding scheme to allow the receiver to identify the phase change in every individual OFDM symbol, we can use single-symbol modulation at the tag and thus double the transmission throughput.

To further increase the throughput of backscatter communication, a tag can backscatter the same excitation signal with two different frequency shifts. We then use two Wi-Fi receivers to capture the backscatter signals on different channels to double the tag throughput.

3.7.2 Dual Receivers

As shown in Fig. 3.1, the MOXcatter system requires two commodity receivers to decode the tag information. Specifically, in Eq. 3.10, one receiver is needed to capture the original data **Q** at the original Wi-Fi channel, and another receiver is needed to obtain the backscattered data **B** at the frequency-shifted backscatter channel. Nowadays, as Wi-Fi infrastructure is highly developed, it is easy to find two commodity devices to deploy the MOXcatter decoder, such as a laptop with a NIC and a cellphone. By recording the timestamps of received packets at both receivers, we ensure that tag data decoding is conducted on the same raw packet but only from different channels. However, if the tag information can be decoded from a single receiver, it would significantly reduce the hardware cost and synchronization overhead in the backscatter system.

3.7.3 Multiple Access Control

We have mainly studied backscatter communication with a single tag. However, a MAC protocol is required to coordinate the channel-sharing issue for the tags in scenarios where multiple tags co-exist, such as an indoor environmental monitoring system with different sensor tags communicating with a Wi-Fi-based hub. One solution is to use control signals to inform the tags of the transmission sequence. Once a tag receives a control signal with a specific ID, it compares it with its own ID. If the IDs match, the tag is enabled to transmit data; otherwise, it backs off. This approach allows all tags to use the same channel for backscatter communication. It's worth noting, however, that a receiver cannot receive backscattered data from multiple tags at the same time. To overcome this, tags can backscatter from different channels and multiple Wi-Fi adapters can receive the backscattered data.

3.8 Summary

This chapter introduces MOXcatter, a backscatter communication system that employs spatial multiplexing in Wi-Fi signals. We overcame the challenges of designing spatial backscatter with off-the-shelf Wi-Fi devices. We build a hardware prototype for the MOXcatter tag. Experimental results show that MOXcatter achieves throughput of up to 50 kbps with single-stream signals and up to 1 kbps with double-stream signals in 802.11n. Our design has great potential in the new generation 802.11 networks. The performance can be improved towards high throughput and lower complexity, possibly with the introduction of Multi-user MIMO (MU-MIMO) technology in advanced Wi-Fi protocols like 802.11ac/ax.

References

1. Bluetooth vs. wi-fi power consumption. https://github.com/wisp/wisp5
2. Gollakota S, Reynolds MS, Smith JR, Wetherall DJ (2013) The emergence of RF-powered computing. Computer 47(1):32–39
3. Kellogg, B, Parks, A, Gollakota, S, Smith, JR, Wetherall D (2014) Wi-fi backscatter: internet connectivity for RF-powered devices. In: Proceedings of the 2014 ACM conference on SIGCOMM, pp 607–618
4. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 356–369
5. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 370–383
6. Abari O, Vasisht D, Katabi D, Chandrakasan A (2015) Caraoke: an e-toll transponder network for smart cities. In: Proceedings of the 2015 ACM conference on special interest group on data communication, pp 297–310
7. Hu P, Zhang P, Rostami M, Ganesan D (2016) Braidio: an integrated active-passive radio for mobile devices with asymmetric energy budgets. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 384–397
8. Kellogg B, Talla V, Gollakota S (2014) Bringing gesture recognition to all devices. In: 11th USENIX symposium on networked systems design and implementation (NSDI'14), pp 303–316
9. Liu V, Parks A, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. ACM SIGCOMM Comput Commun Rev 43(4):39–50
10. Wang A, Iyer V, Talla V, Smith JR, Gollakota S (2017) FM backscatter: enabling connected cities and smart fabrics. In: USENIX symposium on networked systems design and implementation (NSDI), vol 17, pp 3154630–3154650
11. Talla V, Kellogg B, Gollakota S, Smith JR (2017) Battery-free cellphone. Proc ACM Interact Mobile Wearable Ubiq Technol 1(2):1–20
12. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In: 13th $\{USENIX\}$ symposium on networked systems design and implementation ($\{NSDI\}$ 16), pp 151–164
13. Wong MSY, Gilbert JM, Barratt CH (2008) Wireless LAN using RSSI and BER parameters for transmission rate adaptation, 2008. US Patent 7,369,510
14. Pefkianakis I, Hu Y, Wong SHY, Yang H, Lu S (2010) MIMO rate adaptation in 802.11 n wireless networks. In: Proceedings of the sixteenth annual international conference on mobile computing and networking, pp 257–268
15. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM, pp 259–271
16. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of the 13th international conference on emerging networking experiments and technologies, pp 389–401
17. Bharadia D, Joshi KR, Kotaru M, Katti S (2015) Backfi: high throughput wifi backscatter. ACM SIGCOMM Comput Commun Rev 45(4):283–296
18. Gummeson J, Zhang P, Ganesan D (2012) Flit: a bulk transmission protocol for RFID-scale sensors. In: Proceedings of the 10th international conference on Mobile systems, applications, and services, pp 71–84
19. Hassanieh H, Wang J, Katabi D, Kohno T (2015) Securing RFIDs by randomizing the modulation and channel. In: 12th $\{USENIX\}$ symposium on networked systems design and implementation ($\{NSDI\}$ *15)*, pp 235–249
20. Hu P, Zhang P, Ganesan D (2014) Leveraging interleaved signal edges for concurrent backscatter. In: Proceedings of the 1st ACM workshop on Hot topics in wireless, pp 13–18

21. Hu P, Zhang P, Ganesan D (2015) Laissez-faire: fully asymmetric backscatter communication. ACM SIGCOMM Comput Commun Rev **45**(4), 255–267
22. Liu V, Talla V, Gollakota S (2014) Enabling instantaneous feedback with full-duplex backscatter. In: Proceedings of the 20th annual international conference on Mobile computing and networking, pp 67–78
23. Parks, AN, Liu, A, Gollakota S, Smith JR (2014) Turbocharging ambient backscatter communication. ACM SIGCOMM Comput Commun Rev 44(4):619–630
24. Talla V, Kellogg B, Ransford B, Naderiparizi S, Gollakota S, Smith JR (2015) Powering the next billion devices with wi-fi. In: Proceedings of the 11th ACM conference on emerging networking experiments and technologies, pp 1–13
25. Wang J, Adib F, Knepper R, Katabi D, Rus D (2013) RF-compass: robot object manipulation using RFIDs. In: Proceedings of the 19th annual international conference on Mobile computing & networking, pp 3–14
26. Wang J, Hassanieh H, Katabi D, Indyk P (2012) Efficient and reliable low-power backscatter networks. ACM SIGCOMM Comput Commun Rev 42(4):61–72
27. Wang J, Katabi D (2013) Dude, where's my card? RFID positioning that works with multipath and non-line of sight. In: Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, pp 51–62
28. Wang J, Vasisht D, Katabi D (2014) RF-idraw: virtual touch screen in the air using RF signals. ACM SIGCOMM Comput Commun Rev 44(4):235–246
29. Zhang P, Ganesan D (2014) Enabling bit-by-bit backscatter communication in severe energy harvesting environments. In: 11th $\{USENIX\}$ symposium on networked systems design and implementation ($\{NSDI\}$ 14), pp 345–357
30. Zhang P, Ganesan D, Lu B (2013) Quarkos: pushing the operating limits of micro-powered sensors. In: 14th workshop on hot topics in operating system (HotOS)
31. Zhang P, Gummeson J, Ganesan D (2012) Blink. In: Proceedings of the 10th international conference on Mobile systems, applications, and services. ACM, New York
32. Zhang P, Hu P, Pasikanti V, Ganesan D (2014) Ekhonet: high speed ultra low-power backscatter for next generation sensors. In: Proceedings of the 20th annual international conference on Mobile computing and networking, pp 557–568
33. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of the 16th annual international conference on mobile systems, applications, and services, pp 191–203
34. Wireless LAN medium access control (MAC) and physical layer (phy) specifications (1999). IEEE Std 802.11-1999
35. Wireless LAN medium access control (MAC) and physical layer (phy) specifications: high-speed physical layer in the 5 ghz band (1999). IEEE Std 802.11a-1999
36. Wireless LAN medium access control (MAC) and physical layer (phy) specifications, amendment 4: further higher data rate extension in the 2.4 ghz band (2003). IEEE Std 802.11g-2003
37. Wireless LAN medium access control (MAC) and physical layer (phy) specifications, amendment 5: enhancements for higher throughput (2009). IEEE Std 802.11n-2009
38. CommView for WiFi. http://www.tamos.com/products/commwifi/

Chapter 4
Single-Symbol Wi-Fi Backscatter with Uncontrolled Ambient Signals

Abstract The use of controlled excitation makes pervasive backscatter communication difficult to achieve and the redundant modulation severely limits the performance of the system. In this chapter, we first present RapidRider, a novel Wi-Fi backscatter system that can take uncontrolled OFDM Wi-Fi signals, e.g., 802.11a/g/n/ac, as excitations and efficiently embeds tag data at the single-symbol rate. Since uncontrolled Wi-Fi signals are everywhere in our daily life, such a system can bring us closer to the dream of ubiquitous backscatter connection. Specifically, we show for the first time why the previous systems have to rely on multi-symbol modulation. We have a deep look at the Wi-Fi signal processing and discover the fundamental reason, which makes it possible for us to demodulate tag data on the single-symbol level. Further, we design deinterleaving-twins decoding method that can reuse any uncontrolled Wi-Fi signals as carriers to backscatter and demodulate tag data at single-symbol level. Moreover, to accommodate cases where there is only one receiver available, we design RapidRider+, a system that enables us to take productive data and tag data on the same packet by aggregated transmission, which can freely control both data ratios to adapt to different application scenarios. To verify the effectiveness of our proposal, we prototype our system using various FPGAs, commodity radios, and SDRs. Comprehensive evaluations demonstrate that we have achieved single-symbol modulation with guaranteed transmission accuracy on uncontrolled OFDM Wi-Fi signals. The results show that our solution's maximum throughput is 3.92× and 1.97× better than the existing advanced system FreeeRider and MOXcatter. We can achieve an aggregated goodput of productive and tag data around 1 Mbps on average with RapidRider+.

4.1 Introduction

In recent years, with the increase in the number of connected IoT devices, the demand for data transmission has also surged. The huge resource consumption required for wireless communication has become an important issue that cannot be ignored. Backscatter communication, an ultra-low-power data transmission technology, has attracted much attention in wireless sensor networks (WSN) [1–

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_4

10]. A typical backscatter system is RFID, which has been widely used in many scenarios such as logistics tracking, book management, food supervision, etc. [11–14]. Such a system usually consists of two main components, a reader that serves as both the excitations and the receiver, and a tag that takes excitations as carriers and backscatters data to the reader [15–20]. However, dedicated readers are expensive and cannot be widely deployed to meet the needs of large-scale IoT. To address this problem, a seminal work, ambient backscatter using the ambient signals as carriers [1], is proposed. Since then, many researchers are inspired by it and use various ambient signals to achieve backscatter communication, e.g., FM backscatter [21], Wi-Fi backscatter [22–24], Bluetooth backscatter [25, 26], and LoRa backscatter [27]. The common goal is to make backscatter into pervasive ambient communication for the Internet of Things (IoT).

The development of technology often requires a long process. Most of the preliminary work does not really take advantage of the ambient signals, but rather requires tight control of the excitations. A dedicated device is needed to provide single tone as carriers and tags generate standard packets on it, e.g., LoRa [27], Wi-Fi [28], ZigBee [29]. Although those systems can achieve standard-compliant tag data rates, they can only use dedicated excitation sources like single-tone rather than ubiquitous ambient signals. Along this side, some researchers explore new systems that can work with uncontrolled ambient signals to get closer to universal backscatter. Packet-level Wi-Fi backscatter solution comes first by embedding tag data in the signal amplitude changes of packets [23, 30], which means that it can only carry one-bit tag data per packet. The most recent advances have increased the data rate to some extent. FreeRider [26] and MOXcatter [31], can transmit the tag data based on ambient OFDM Wi-Fi signals at symbol-level. However, they still suffer from three main drawbacks.

1. *Redundant modulation*. To ensure satisfactory BERs for the receiver, a majority of previous techniques adopt a strategy of employing multi-symbol modulation for tag data. For example, FreeRider [26] modulates a tag bit using four OFDM symbols, and MOXcatter [31] does so with every two OFDM symbols. When using single-symbol modulation for tags, those systems would fail and exhibit high BERs. Such redundancy leaves much room for throughput improvement.
2. *Constrained ambient excitations*. Embedding tag data onto legitimate Wi-Fi is the goal for ambient Wi-Fi backscatter. The previous systems add a number of constraints on excitations to achieve this goal. For example, Passive Wi-Fi [28] can only use continuous waves (CWs) as excitations, which are provided by an extra helper device. Interscatter [29] relies on the single-tones as carriers, which are produced by de-whitened Bluetooth signals. MOXcatter [31] exclusively supports Wi-Fi excitations that carry a payload consisting entirely of either 0s or 1s. Therefore, using uncontrolled Wi-Fi signals as carriers and achieving single-symbol level modulation is still a challenging problem.
3. *Inconvenient two-receiver demodulation*. Hitchhike [24] opens the door to using productive data as excitations. A number of works have been inspired by [24] and made further contributions, e.g., MOXcatter [31], X-tandem [32]. However, those

systems still suffer from a common limitation that two receivers are needed to demodulate tag data. Such a redundancy not only increases the system hardware cost but requires accurate synchronization of two separate receivers.

In this chapter, we propose RapidRider, a new Wi-Fi backscatter system that can efficiently embed tag data on uncontrolled OFDM Wi-Fi signals at the single-symbol level. We will first show why current systems cannot modulate tag data at the single-symbol level. Subsequently, we present our single-symbol solution by taking advantage of deinterleaved data. Additionally, we devise a deinterleaving-twins decoding scheme that encompasses both forward and backward deinterleaving processes to enable the use of uncontrolled excitations. Further, we present RapidRider+, a single-receiver solution by using a novel aggregate transmission mechanism that enables the transmission of both productive data and tag data within the same packet. Consequently, a single receiver is sufficient for decoding both data and we can overcome the limitation of relying on two receivers.

Through comprehensive experiments, RapidRider demonstrates its resilience across a wide range of environments, encompassing both LoS and NLoS scenarios, various excitation signals and frequencies, different excitation rates, as well as in the presence of interferences. The main performances of the systems are summarized below:

1. The maximum throughput of RapidRider in LoS scenarios is 1.97× better than MOXcatter and 3.92× better than FreeRider.
2. The BER of RapidRider could be as low as 1.3% for single-symbol modulation, While that of FreeRider is 43%.
3. When using only one receiver, the aggregate goodput of productive and tag data for RapidRider+ can achieve 1 Mbps on average.

4.2 Related Work

In recent years, a large number of backscatter systems that take advantage of various popular RF radios came out, e.g., Wi-Fi backscatter [22, 28], Bluetooth backscatter [25], LoRa backscatter [27], and FM backscatter [21]. Among them, Wi-Fi backscatter has garnered significant attention since Wi-Fi is the most popular and abundant one.

In recent years, extensive research has been conducted on Wi-Fi backscatter systems, leading to significant advancements. Some works contribute to reducing the redundancy of modulation. The initial backscatter system implemented packet-level modulation resulting in extremely low data rates, such as FS Backscatter [23], Wi-Fi Backscatter [30] and so on. Subsequently, some novel solutions are proposed to further advance the modulation granularity, pushing it to the sub-packet level. Backfi [22], Passive Wi-Fi [28] and Wi-Fi Backscatter [30] achieve higher rates by using some dedicated devices or specialized hardware, which are used to generate specific carriers like single-tones. However, it is obvious that the special

devices not only increase the system cost but cannot make full use of the existing RF radios. Later, a pioneering work, HitchHike [24] realize a Wi-Fi backscatter system compatible with commercial equipment by codeword translation and achieve symbol-level demodulation. Work along this line, FreeRider [26] can modulate one tag bit on four symbols and MOXcatter [31] can modulate one tag bit on two symbols. What's more, for the systems using codeword translation as modulation and demodulation methods, they need two receivers to capture the backscatter data and original data, separately. In short, they still cannot achieve single-symbol level modulation on uncontrolled OFDM Wi-Fi signals. Based on the above works, [33] is trying to further push the limits of modulation granularity. We first identify the fundamental reasons for the incompatibility challenge between OFDM Wi-Fi operations and codeword translation. Then, an innovative deinterleaving-twins decoding approach are proposed that achieves the single-symbol level modulation and ensures optimal performance.

4.3 Wi-Fi Backscatter Background

4.3.1 OFDM Wi-Fi

In Sect. 3.3.1, we have introduced a typical spatial stream transmission for Wi-Fi. In this chapter, we will focus on the single-stream transmission process. Although there are a series of modulation techniques in Wi-Fi family, OFDM (orthogonal frequency-division multiplexing) Wi-Fi is becoming more popular in recent years for its higher throughput and anti-interference.

Figure 4.1 shows the basic architecture at the physical layer for OFDM Wi-Fi protocol. Some of them are the same as that of the spatial stream in Sect. 3.3.1. Here we do a brief review. The input data is a bitstream. The first step is padding some data fields including SERVICE, TAIL, and PAD to make the bitstream ready for the later OFDM processing. Afterward, the data passes through a scrambler designed to convert the original bitstream into a random sequence that avoids being exclusively composed of zeros or ones. Channel encoding enhances the robustness of the scrambled bitstream against channel interference by error correction. In most OFDM Wi-Fi, BCC (binary convolutional code) is used for data encoding. Additionally, the interleaver further improves the system's anti-interference capabilities by employing permutations to handle burst errors. Once the bit-level operations are

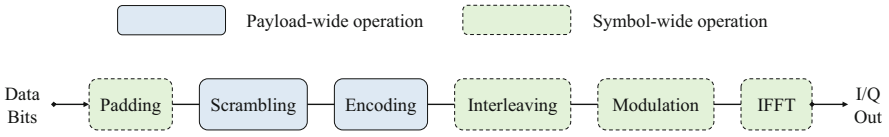


Fig. 4.1 Transmitter operations for OFDM Wi-Fi signals

completed, a constellation mapper then modulates the data bit 0 or 1 to a complex number. There are a lot of modulation modes, such as BPSK, QPSK, QAM, and so on, which correspond to different data rates. Finally, the data is then transformed from the frequency domain to the time domain using the IFFT (inverse fast Fourier transform) operation, ensuring orthogonality among the subcarriers.

In addition to the functions of the individual operations, we are more concerned with the scope of their operation. These operations can be mainly classified into two categories: payload-wide and symbol-wide. Symbol-wide operations, such as padding, interleaving, modulation, and IFFT, are confined to individual symbols without affecting others. On the other hand, scrambling and encoding are payload-wide operations, as they impact the entire payload.

4.3.2 Codeword Translation

Section 3.3 has given a detailed description of the principles of codeword translation including the design of the tag codebook and the demodulation method. In this chapter, we use BPSK for tag data modulation. In this case, we have two codewords, $C_1 = e^{j\theta_1}$, $C_2 = e^{j\theta_2}$, where $\theta_1 - \theta_2 = \pi$. We rotate π on the former codeword C_x when transmitting the tag data $t_x =$ '1'. The backscatter data can be expressed as $C'_x = C_x \cdot e^{j\pi}$, which is still a valid codeword. If the tag data $t_x =$ '0', we keep the current codeword unchanged. Therefore, at the receiver, the tag bit can be decoded by performing a simple XOR operation.

$$C_x \oplus C'_x = t_x \tag{4.1}$$

The phase-based codeword translation on OFDM Wi-Fi is a symbol-wide operation. Despite its ease of implementation, codeword translation encounters several drawbacks. The biggest problem is that the current systems highly rely on redundant modulation due to the burst [31] errors or interference from existing OFDM Wi-Fi processing operations [26]. In this chapter, we find the fundamental reason for inter-symbol errors first and then present our solution.

4.4 RapidRider Design

4.4.1 Overview

The framework of RapidRider is shown in Fig. 4.2. For the transmitter, we use ambient Wi-Fi signals as excitations and send the signals on channel A. The tag employs single-symbol modulation on the excitations. At the same time, the backscattered signals are shifted to a different Wi-Fi channel B to avoid interference.

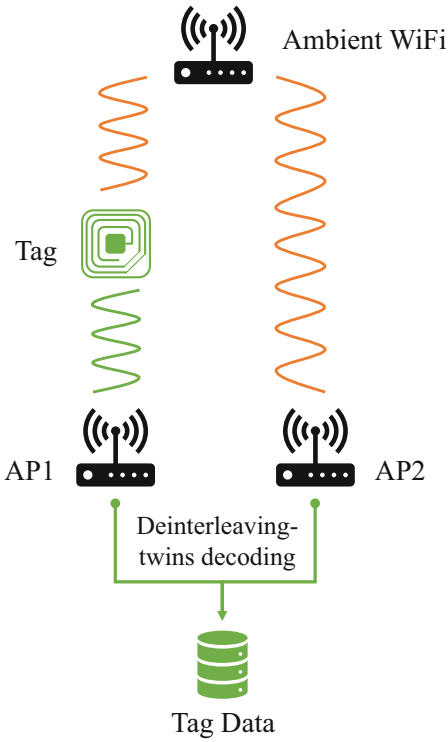


Fig. 4.2 The framework of RapidRider

At the receiver, two APs (Access Points) are used to receive the original data in channel A and the backscattered data in channel B, separately. Different from the previous works that recover the tag data by XOR the payload data, we propose a novel deinterleaving-twins decoding method that can successfully recover the tag data with a low BER. There are two main challenges to achieving the above idea: (1) how to modulate and demodulate the tag data at the single-symbol level? (2) how can the system effectively handle uncontrolled ambient signals?

4.4.2 Single-Symbol Modulation

We first represent the whole backscatter procedure in a formal way. At the transmitter, the Wi-Fi operations padding, scrambling, encoding, interleaving, modulation, and IFFT can be denoted as $\mathcal{T}_p$, $\mathcal{T}_s$, $\mathcal{T}_e$, $\mathcal{T}_i$, $\mathcal{T}_m$, and $\mathcal{T}_{IFFT}$, respectively. Then we can express the Wi-Fi transmission process as below.

$$\mathcal{T}(\cdot) = \mathcal{T}_{IFFT}(\mathcal{T}_m(\mathcal{T}_i(\mathcal{T}_e(\mathcal{T}_s(\mathcal{T}_p(\cdot)))))), \tag{4.2}$$

We denote the payload at the transmitter as $t = (t_1, t_2, \ldots, t_n)$. Then the transmitted data can be expressed as $\mathcal{T}(t)$. We denote the tag signals as $s = (s_1, s_2, \ldots, s_n)$ and the codeword translation as C. Then the backscattered signals, b, can be represented as the time-domain product of the tag signals and excitations.

$$b = C(\mathcal{T}(t), s) = (\mathcal{T}(t)_1 \oplus s_1, \ldots, \mathcal{T}(t)_n \oplus s_n), \tag{4.3}$$

At the receiver in channel A, the AP captures the original signal and can recover the payload data t correctly. At the receiver in channel B, the backscattered signals will undergo a series of reverse processing denoted as $\mathcal{T}^{-1}(\cdot)$ to demodulate payload data. We denote the demodulated the backscattered payload as $r = (r_1, r_2, \ldots, r_n) = \mathcal{T}^{-1}(b)$. Therefore, we can decode the tag data, $\hat{s} = (\hat{s}_1, \hat{s}_2, \ldots, \hat{s}_n)$, by t and r.

$$\hat{s} = C^{-1}(t, r) = (t_1 \oplus r_1, \ldots, t_n \oplus r_n) \tag{4.4}$$

Everything seems perfect, however, it has been proved that $t_i \oplus r_i = \hat{s}_n \neq s_i$. The underlying issue lies in the fact that only when the Wi-Fi operations $\mathcal{T}$ are commutative with codeword translation C, can we get that $t_i \oplus r_i = s_i$. The commutative property means for two functions g and f, $g(f(\cdot)) = f(g(\cdot))$. Therefore, the key issue now is to analyze the relationship between $\mathcal{T}$ and C.

Let us take a deep look at the above operations. To finally decode tag data, it will go through several processes including Wi-Fi transmission $\mathcal{T}$, codeword translation C, inverse Wi-Fi transmission $\mathcal{T}^{-1}$, and decodeword-translation C^{-1}.

$$\hat{s} = C^{-1}(\mathcal{T}^{-1}(C(\mathcal{T}(t), s)), t) \tag{4.5}$$

It is evident that if $\mathcal{T}$ and C are commutative, $\hat{s} = \mathcal{T}^{-1}(C^{-1}(C(\mathcal{T}(t), s), t))$. Then C and C^{-1}, $\mathcal{T}$ and $\mathcal{T}^{-1}$ are cancelled with each other, $\hat{s} = t$. Unfortunately, after analyzing, we find that $\mathcal{T}$ and C are not commutative, which means that $\hat{s} \neq s$. We present a toy example in Fig. 4.3. Figure 4.3a shows that the input data t is (0x000000, 0x000000). After a series of operations, the expected data s is (0xFFFFFF, 0x000000), while the decoded data $\hat{s}$ is (0x17FFC5, 0x000000). Figure 4.3b further illustrates that $\mathcal{T}$ and C do not commute with each other since $C(\mathcal{T}(t), s) \neq \mathcal{T}(C(t, s))$.

Therefore, it is challenging to do single-symbol level demodulation on OFDM signals. To avoid this problem, the previous works, like FreeRider [26] and MOXcatter [31], choose to do tag modulation on the multi-symbols level. The redundancy limits the transmission data rate greatly. Fortunately, we have found the fundamental reason preventing the implementation of single-symbol modulation is the non-commutativity between $\mathcal{T}$ and C.

Based on this insight, when only keeping the Wi-Fi operations that are commutative with codeword translation C, we can realize the single-symbol demodulation. From Fig. 4.1, we can know that the Wi-Fi operations after interleaving are all

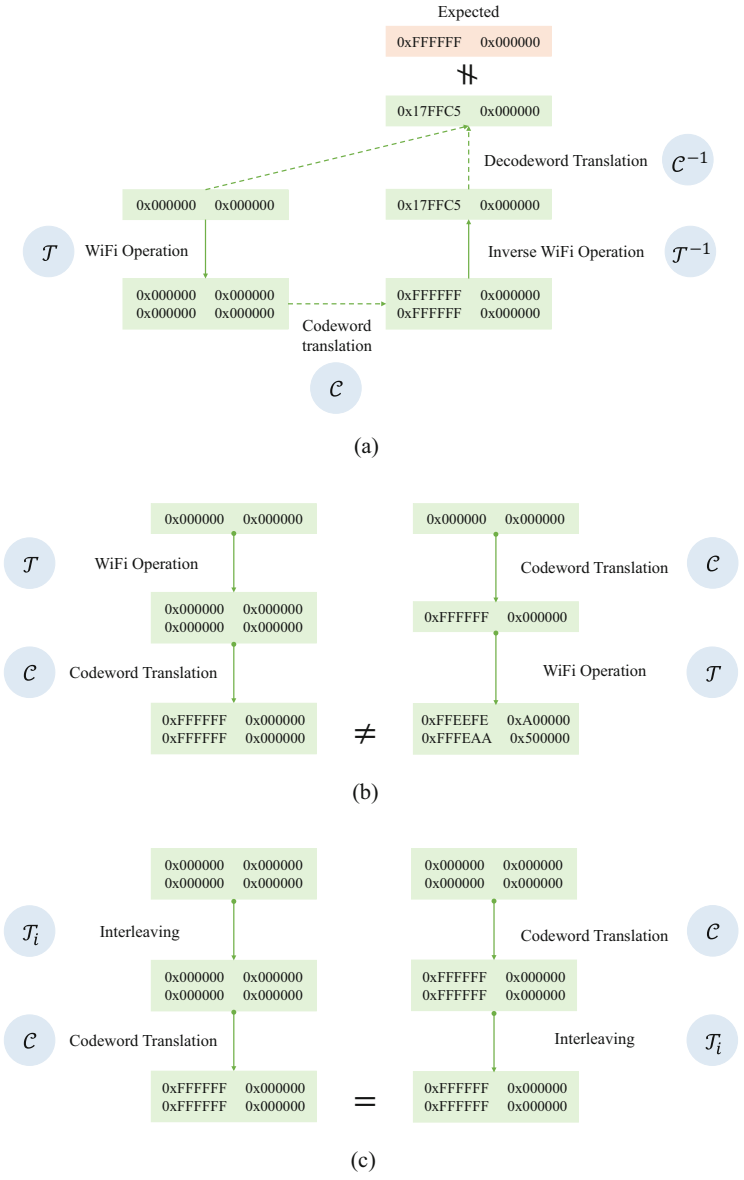


Fig. 4.3 A toy example of backscatter decoding process. (**a**) Backscatter decoding process. (**b**) $\mathcal{T}$ and C are not commutative. (**c**) $\mathcal{T}_i$ and C are commutative

symbol-wide. When we do data decoding, we should go through the inverse operations which are IFFT, Demodulation, and Deinterleaving. It can be proved that these operations and the inverse ones are commutative with C. First, since IFFT (or FFT) $\mathcal{F}$ is a linear function, if $\mathcal{F}(x_n)_k = X_k$, then $\mathcal{F}(ax_n)_k = aX_k$, where

a is any complex number and k is the index. For OFDM Wi-Fi signals, we do phase rotation for codeword translation which means that $a = e^{j\theta}$. Therefore, $\mathcal{F}$ is commutativity with C. Second, because the modulation and demodulation operations entail a straightforward one-on-one mapping process and C is applied to all constellation points, they are also commutative with C. Finally, interleaving and deinterleaving operations re-order the bitstream at symbol-wide, which means that there is no cross-symbol interference. In short, these three operations are all commutative with C, so $\mathcal{T}'$ is also commutative with C as shown in Fig. 4.3c.

4.4.3 Deinterleaving Decoding

Thus, we propose a deinterleaving-based decoding method and denote it as $\mathcal{T}'(\cdot) = \mathcal{T}_{IFFT}(\mathcal{T}_m(\mathcal{T}_i(\cdot)))$. The basic idea is to work at the deinterleaved-data level instead of the payload level. The details are as follows.

First, we apply 2 forward interleavers at two receivers. The obtained Wi-Fi signals (original signal and backscattered signal) only go through three symbol-wide operations, FFT, Demodulation, and Deinterleaving. Then we can recover the tag data by employing XOR (decodeword-translation C^{-1}) on the two deinterleaved bitstreams. We denote the data before interleaving as $t' = \mathcal{T}_e(\mathcal{T}_s(\mathcal{T}_p(t)))$. Since $\mathcal{T}'$ is commutative with C, it is easy to prove that the recovered tag data $\hat{s'}$ is the same as the expected one s.

$$\hat{s'} = C^{-1}(\mathcal{T}'^{-1}(C(\mathcal{T}'(t'), s)), t') \tag{4.6}$$

$$= C^{-1}(\mathcal{T}'^{-1}(\mathcal{T}'(C(t', s))), t') \tag{4.7}$$

$$= C^{-1}(C(t', s), t') \tag{4.8}$$

$$= s. \tag{4.9}$$

4.4.4 Deinterleaving-Twins Decoding

Although the above scheme works well in principle, in practice there is a problem: the bitstreams at the deinterleaving layer are not available through the commercial NIC. Commercial devices, such as routers, smartphones, etc., only have access to payload data. However, it has been proven that we cannot do single-symbol modulation on the payload level. It seems that the SDRs (software defined radio) are needed to capture data at the interleaving level. However, the application of SDRs increases the cost of the system and is not conducive to widespread deployment, so what we want is to be able to use existing commercial equipment. To achieve this goal, we propose a deinterleaving-twins solution with the insight that we can reuse the recovered payload data from commercial AP.

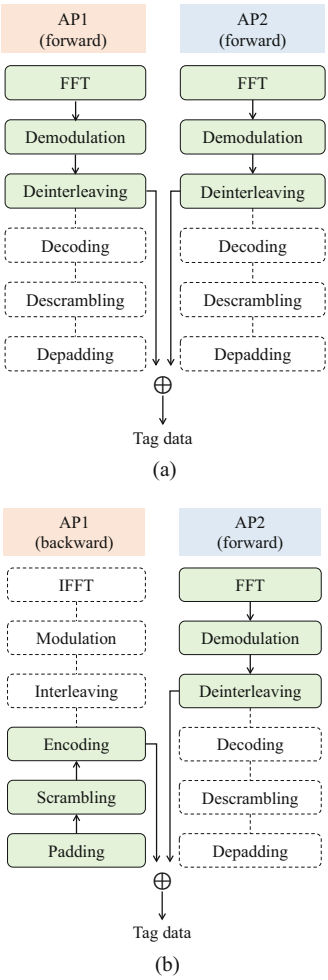


Fig. 4.4 The schemes of deinterleaving decoding and deinterleaving-twins decoding. (**a**) 2 forward deinterleavers. (**b**) 1 forward deinterleaver and 1 backward interleaver

We define 1 forward deinterleaver, and 1 backward deinterleaver as shown in Fig. 4.4. The backward one for unchanged payload data from a commercial NIC (AP1) goes through the three operations in the opposite direction, padding, scrambling, and encoding. The forward one for received IQ data from backscattered signals (AP2) goes through the same operations as the former method. Due to the invertibility of all Wi-Fi operations, it can be easily demonstrated that a forward deinterleaver and a backward interleaver are expected to produce identical deinterleaved data.

$$\mathcal{T}_i^{-1}(\mathcal{T}_m^{-1}(\mathcal{T}_{IFFT}^{1}(\hat{t}))) = \mathcal{T}_e(\mathcal{T}_s(\mathcal{T}_p(t))), \hat{t} = \mathcal{T}(t). \tag{4.10}$$

Everything seems perfect, however, a challenge lies in the backward deinterleaver: we can get the scrambler seed from the commercial NIC, and the seed is crucial for the scrambling process. Our insight here is that the scrambler seeds for the two receivers are the same as long as we remain this data part unchanged when doing codeword translation. Since the scrambler seed is at the beginning fields of the payload, what we should do is skipping these fields. In this way, we can recover the scrambler seed by AP2 and AP1 can use this seed to generate the interleaving data by recovered payload data. Finally, we can decode the tag data by simple XORing operations.

4.5 RapidRider+ Design

Although we can recover the tag data successfully now, the current systems encounter a significant challenge: two receivers are needed to decode tag data This requirement presents three notable drawbacks: (1) It introduces additional synchronization overhead between the two receivers to ensure accurate decoding. Because the XOR decoding operation we use is a bit-by-bit operation, the synchronization requirements are extremely high. (2) It relies on obtaining data from ambient signals by an-extra commercial NICs, which is not always readily accessible. (3) To avoid two signals interfering with each other, we shift the backscatter signals to another channel. Occupancy of two channels reduces spectrum efficiency. In light of these limitations, we have developed RapidRider+, a backscatter scheme that enables the transmission of both productive and tag data within the same packet, thereby eliminating the need for two receivers. With this scheme, a single receiver is sufficient for decoding both types of data, optimizing the overall system efficiency.

4.5.1 Single-Receiver for Aggregated Transmissions

The main design for RapidRider+ is about excitation. Our key insight is that the key to codeword translation is the reference for decoding. Therefore, as shown in Fig. 4.5, the excitation Wi-Fi signal of RapidRider+ contains two parts: productive data and carrier part. The former part is dedicated to transmitting productive data, where the symbols can be arbitrary. Notably, the last symbol of the first part is

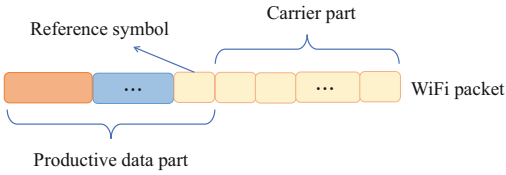


Fig. 4.5 The packet structure design of RapidRider+

designated as the reference symbol. The carrier part consists entirely of reference symbols, which is for codeword translation. Since all the symbols in the carrier part are the same, it can be considered as a special 'continuous wave'. The encoding and decoding processes of RapidRider+ are introduced below.

Encoding To ensure the single receiver can know the original data, the reference symbol should not be affected. Therefore, after detecting the excitation signals, the tag jumps over the productive data part of the payload, which means that no phase shift is conducted. Then the tag put data onto the carrier signal by phase-based codeword translation. Instead of multi-symbol modulation, We embed one tag bit on a single symbol. In this manner, the single packet contains both types of data: productive data and tag data.

Decoding At the receiver, we only need one device to do data decoding. The decoding processes are the same as normal processing the signal sequentially from the preamble to the payload. After recovering the payload data in the productive data part, we can get the reference symbol. when reaching the carrier part, the AP decodes the tag data by performing XOR operations between the last symbol of the productive data segment and each symbol in the carrier part. Consequently, both the productive data and the tag data are successfully recovered as the packet reaches the end.

Since both the productive and tag data are aggregated in one packet, it allows for achieving various trade-offs between these two types of data by adjusting the lengths of the two parts. We denote the total length of the payload as l, and the length of the productive data part as l_p. The aggregated transmission coefficient is defined as $\gamma = \frac{l_p}{l}$. Therefore, depending on the specific requirements of different applications, we have the flexibility to adjust the parameter γ to achieve the desired balance between the two types of data.

4.6 Performance Evaluation

In this section, we briefly introduce the implementation of our system first and then thoroughly assess the performance of RapidRider and conduct a comprehensive comparison with state-of-the-art approaches in diverse environments. Our evaluation begins with measuring the end-to-end performance, followed by conducting micro-benchmark experiments.

4.6.1 Implementation

We prototype RapidRider and RapidRider+ using FPGAs, commodity radios, and USRPs. We use Dell laptops equipped with a Qualcomm Atheros AR938x as

ambient excitations. Our tag consists of three main parts: a signal detector that is constructed by an amplifier AD8313 and a comparator TLV3501, an FPGA XILINX Artix-7 XC7A35T, and an RF switch ADG902. We use two types of devices as receivers. One is the commercial AP the same as the transmitter, and the others are USRP N210 with an SBX40 daughter board and a USRP B210.

4.6.2 Evaluation

In this section, we compare our system to two leading systems, FreeRider [26] and MOXcatter [31]. FreeRider adopts a four OFDM symbol encoding scheme for each tag bit, whereas MOXcatter utilizes two symbols for the same purpose. We do tag modulation at the single-symbol level.

4.6.2.1 RapidRider

End-to-End Experiments
We first measure three main end-to-end performances, RSSIs, BERs, and throughputs, of the backscatter systems. To evaluate performance in different environments, we carry out experiments in both LoS and NLoS scenarios. The backscatter tag is deployed at a distance of 0.5 m from the excitation source. The receiver is moved far away from the tag at different distances.

RSSI Figures 4.6a and 4.7a illustrate that the RSSI of the backscattered signal experiences a rapid decline as the distance increases. When RSSI is too low, it's hard to recover the data from such a weak signal. The maximum communication range for LoS is 14 m, while that for NLoS is 11 m. This discrepancy arises due to the weaker signal strength of backscattered signals in NLoS environments compared to LoS environments. Specifically, for the same distances, RSSIs in NLoS environments exhibit a 5–10 dBm lower value compared to LoS scenarios. Since RSSI serves as an indicator of signal strength, the three backscatter systems do not exhibit significant differences in this aspect.

BER The comparison results of BERs are shown in Figs. 4.6b and 4.7b. For both LoS and NLoS scenarios, BERs increase as the receivers move far away from the tag and are generally better in LoS compared to NLoS. One of the reasons is that the RSSI in NLoS is lower than Los making data decoding more challenging. The BERs of RapidRider achieve below 10% in LoS environments within a distance of 8 m between the receiver and in NLoS one within 5 m. Additionally, in both LoS and NLoS scenarios, FreeRider consistently exhibits lower BERs compared to RapidRider and MOXcatter. This notable difference can be attributed primarily to the employment of redundant coding in FreeRider. However, this redundancy significantly reduces data rates.

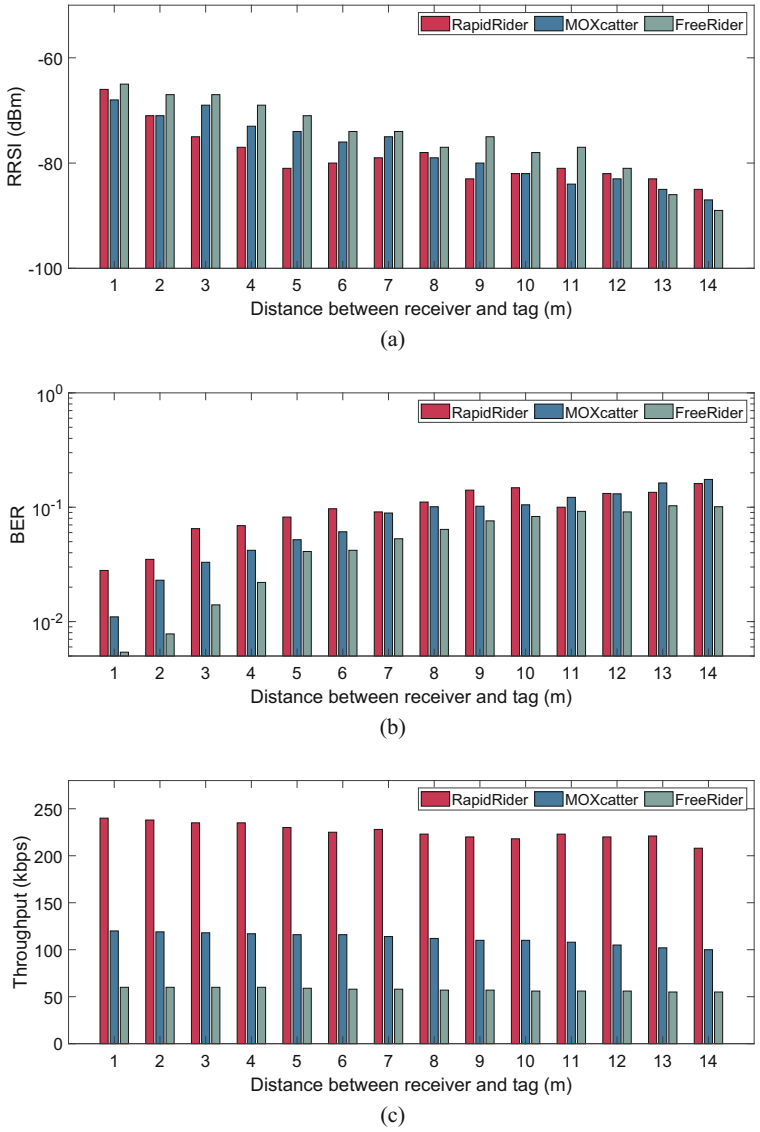


Fig. 4.6 Backscatter transmission performance across distances in LoS scenarios. (**a**) RSSI comparison. (**b**) BER comparison. (**c**) Throughput comparison

Throughput Although the redundant coding reduces the BERs for FreeRider and MOXcatter, they fall short when compared to RapidRider in terms of throughput. Figures 4.6c and 4.7c demonstrate that RapidRider achieves maximum throughputs of 237.8 kbps in LoS scenarios, while those of FreeRider and MOXcatter are 120.8 kbps and 60.7 kbps, respectively. RapidRider outperforms MOXcatter and

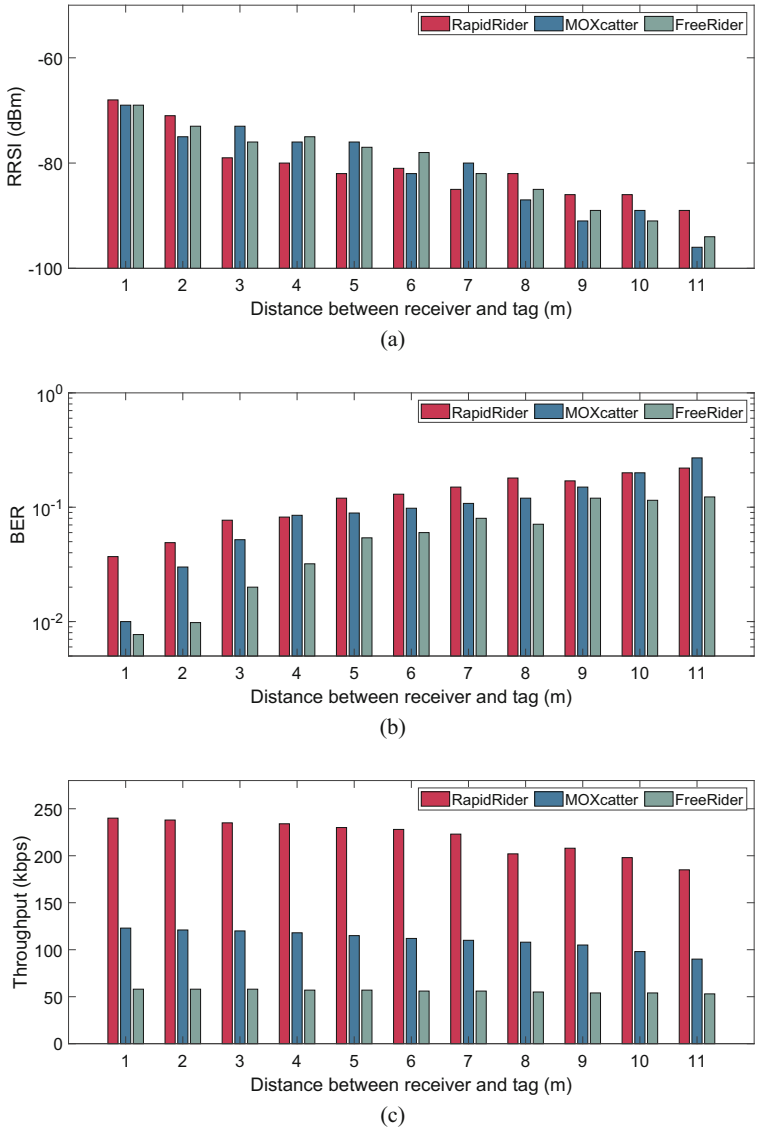


Fig. 4.7 Backscatter transmission performance across distances in NLoS scenarios. (**a**) RSSI comparison. (**b**) BER comparison. (**c**) Throughput comparison

FreeRider by 1.97× and 3.92× in terms of maximum throughput Experimental results are close to the theoretical results, which are 2× and 4× since we modulate at single-symbol, while MOXcatter and FreeRider do so on two symbols and four symbols. In the NLoS scenarios, the results are similar to the above.

Impact of Single Symbol Modulation
Subsequently, we evaluate the performance of RapidRider's single-symbol encoding. Here we introduce a new assessment indicator goodput, which represents the application-layer throughput, influenced by various factors beyond the physical-layer throughput. It serves as another crucial metric for evaluating communication and networking systems. In this section, we focus on the examination of the behavior of RapidRider and FreeRider in the context of single-symbol modulation. We measure the BERs and goodput for different distances and excitation rates as follows.

Distance We put the tag 1 m away from the receiver and test the impact of the distance from the tag to the transmitter on system performance. The transmitter is fixed at distances of 0.3 and 1 m from the tag. In this manner, we choose the excitation rate at 500 pkt/s. From Fig. 4.8a, we can know that when the distance between tag and transmitter is 0.3 m, the BERs of RapidRider and FreeRider are 1.3% and 43%, respectively. Upon increasing the tag's distance to 1 m from the transmitter, RapidRider's BER experiences a slight rise to 3%, while FreeRider's BER escalates significantly to 79%. The high BERs in FreeRider indicate that the single-symbol decoding cannot work well in such previous systems. Thanks to the low BERs, the goodput of RapidRider is much higher than FreeRider as shown in Fig. 4.8b. When the distance is set to 1 m, the RapidRider's goodput is 38.9 kbps which is 4.7× that of FreeRider. The better performance for RapidRider is due to the deinterleaving-twins method.

Excitation Rate Next, we proceed to examine the impact of different excitation rates. We set three excitation rates 100, 500, and 1000 pkt/s, and fix the distance between the tag and transmitter at 1 m. As depicted in Fig. 4.8c, RapidRider exhibits BERs of 4.1%, 3%, and 2.6% across various excitation rates, while the BERs for Freerider are all over 76%. The increase in rate will cause a slight decrease in BER, but will not affect too much. Figure 4.8d demonstrates that the goodput of RapidRider increases from 7.7 to 78.5 kbps with the excitation rate increasing from 100 to 1000 pkt/s. In contrast, the goodput of FreeRider is still below 20 kbps when the excitation rate reaches 1000 pkt/s. Consequently, we conclude that the excitation rate plays a pivotal role as one of the dominant factors affecting goodput.

4.6.2.2 RapidRider+

Impact of Aggregated Transmission Coefficient This section will investigate the effects of different γ values and their tradeoffs. Here, only one receiver is used to decode the tag data. We maintain a fixed distance of 0.3 m between the excitation transmitter and the backscatter tag, while the receiver is positioned 1 m away from the tag. We fix the excitation rate at 1000 pkt/s and set the values for γ as 1/3, 1/2, and 2/3. The empirical results are presented in Fig. 4.9.

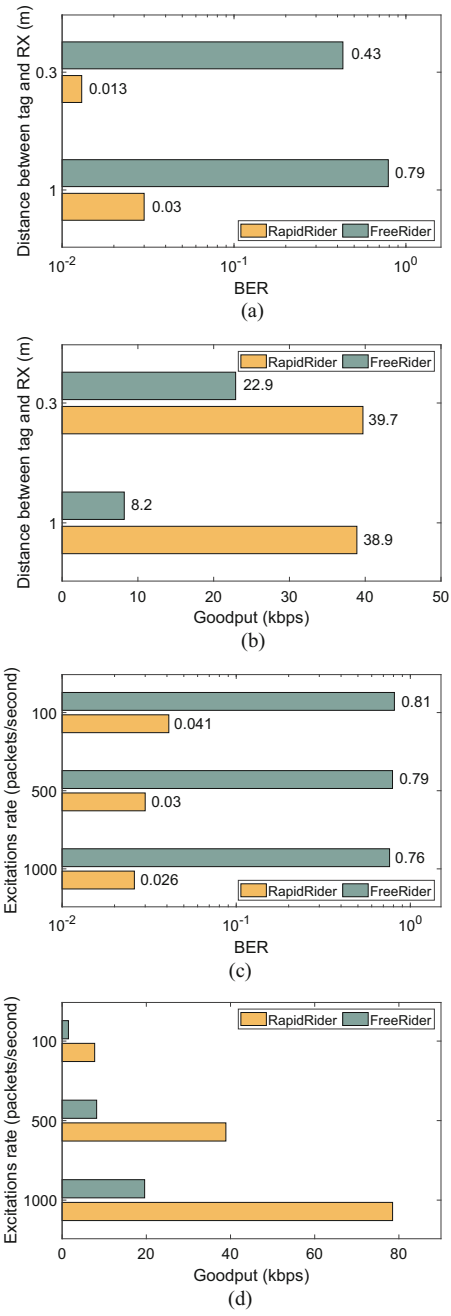


Fig. 4.8 System performance comparison for FreeRider (single-symbol mode) and RapidRider. (**a**) BER comparison at different distances between Tx and tag. (**b**) Goodput comparison at different distances between Tx and tag. (**c**) BER comparison at different excitations rate. (**d**) Goodput comparison at different excitations rate

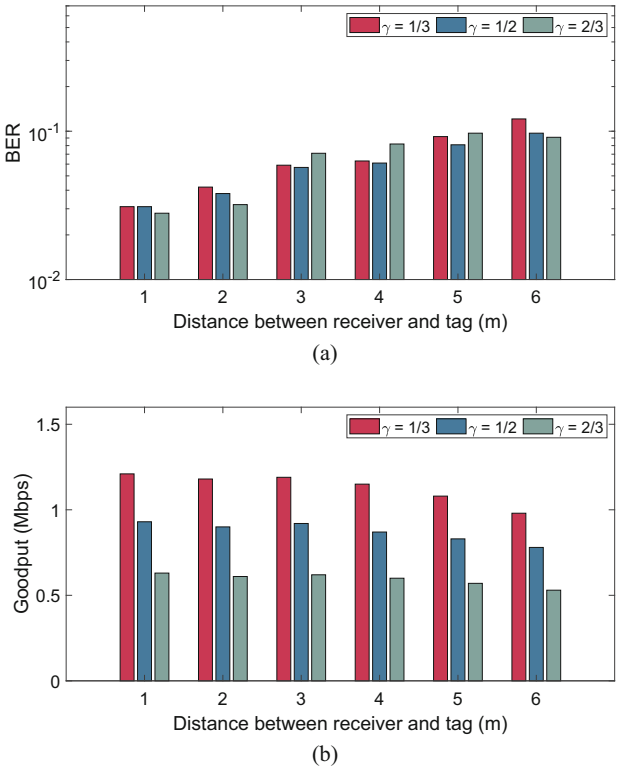


Fig. 4.9 Performance comparison of RapidRider+ in three different modes. (**a**) BER of RapidRider+. (**b**) Aggregate goodput of RapidRider+

As illustrated in Fig. 4.9a, BERs exhibit remarkable stability across various γ settings and are below 10% within 6 m. Turning the attention to goodput, as depicted in Fig. 4.9b, the aggregate goodput reaches 698.6 kbps when γ is set to 1/3. For γ values of 1/2 and 2/3, the corresponding aggregate goodputs are 950.9 and 1243.5 kbps, respectively. These findings highlight that RapidRider+ achieves commendable goodputs for data transmissions. Additionally, by selecting an appropriate γ value, users can make tradeoffs to suit their specific requirements.

Impact of Obstacles Another advantage for RapidRider is supporting a single receiver. The previous systems that relied on two receivers are working on two different channels, an original channel, and a backscatter channel. The system can only work well when both channels are stable and the original and backscatter data can be received and decoded correctly. However, in wireless communications, interference is inevitable. When there is interference on any of the two channels and the data cannot be decoded correctly, the tag data cannot be decoded correctly. RapidRider avoids this problem to a certain extent because it uses only one channel and does not rely on data from other channels.

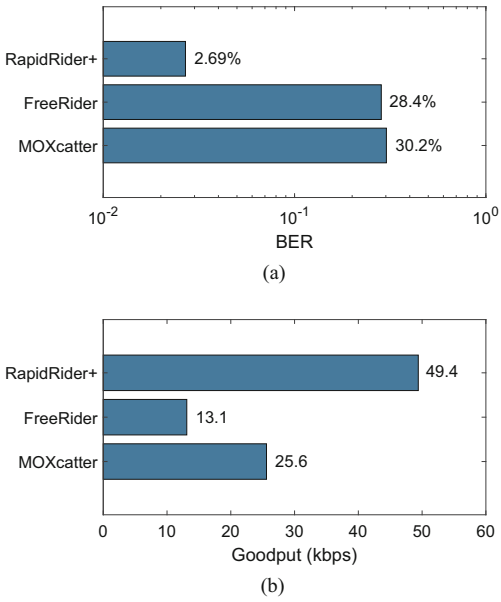


Fig. 4.10 Performance comparison when the original channel is blocked and the backscatter channel is clear. (**a**) Comparison of BER. (**b**) Comparison of Goodput

Therefore, this section measures the impact of the original channel quality on tag data decoding for three systems: RapidRider+, FreeRider, and MOXcatter. We set some metal obstacles on the original channel and keep the bacKscatter channel LoS. The tag is put 0.5 m away from the transmitter and receiver. The excitation rate was set to 1000 pkt/s, and γ was chosen as 1/3. We compare the goodput for tag data transmissions in Fig. 4.10.

Figure 4.10a shows that the BERs of FreeRider and MOXcatter experience significant increases to 28.4% and 30.2%, respectively, while RapidRider+'s BER remains low at only 2.69%. This stark difference proves that the presence of metal obstacles has a detrimental effect on the quality of the original channel, further deteriorating the decoding of tag data. RapidRider+ only requires a single receiver with a clear LoS channel, while the original channels for FreeRider and MOXcatter are obstructed. So RapidRider+ works better when there are obstacles in the original channels. Furthermore, RapidRider+ achieves a higher tag-data goodput compared to both FreeRider and MOXcatter. As illustrated in Fig. 4.10b, RapidRider+ achieves a goodput of 49.4 kbps, whereas FreeRider and MOXcatter only achieve 13.1 kbps and 25.6 kbps, respectively. The reason is that if the original data packet is entirely lost, no tag data can be derived even with perfectly functioning backscatter channels. Thus, the single-receiver solution offered by RapidRider+ demonstrates greater robustness in mobile wireless environments.

4.7 Application Case

Backscatter systems have a wide range of applications due to their specific low power consumption. Our proposed approach greatly improves the throughput on top of existing systems, making more applications possible. Here, we present an application case.

4.7.1 Office Check-In

The previous system was limited by the data rate and could only transmit a very small amount of data. Thanks to single-symbol modulation, the RapidRider can achieve throughput rates of over 200 kbps. This allows us to transfer images. In today's office scenario, attendance statistics rely on employees signing in manually. Often, employees forget to sign in due to negligence, which can lead to unnecessary problems. RapidRider provides a promising solution for office check-in. We can employ tags with ultra-low-power cameras on the wall in the office. The camera regularly captures scenes in the office and uploads them to the system via tags. Attendance can be counted by analyzing the presence of people at each workstation.

4.7.2 Railway Inspection

The railway is one of the most important modes of transport. Staff need to carry out regular inspections of the rails to ensure the safety of train operations. Usually, staff needs to check the state of the railway by tapping, listening, etc., point by point. To simplify the burden on personnel, a large number of sensors are deployed on the track to obtain information. In this case, we have to use battery-free nodes because the dependence of active devices on batteries increases the burden on people to replace them for servicing. Compared to existing systems that require two receivers, our system greatly reduces the burden on employees. Our system supports a single receiver, so that workers can automatically receive information when they pass the node with just one device in their hands.

4.8 Summary

In this chapter, we first present RapidRider, a pioneering Wi-Fi backscatter system that achieves an impressive throughput of 237.8 kbps using ambient OFDM signals. The key innovation lies in its single-symbol decoding scheme, which takes advantage of deinterleaving-twins decoding method. The design of this decoding

scheme is rooted in our realization that some OFDM Wi-Fi operations are not commutative with codeword translation. Then, we represent RapidRider+, a single-receiver solution based on an aggregated transmission mode. We can freely control the proportion of productive and tag and avoid the effects of channel interference on system decoding to some extent. To validate our approach, we implemented a prototype using readily available devices and custom-designed tags. Extensive experiments demonstrate that RapidRider outperforms FreeRider and MOXcatter with remarkable throughput gains of up to 3.92× and 1.97×, respectively. The goodput for RapidRdier+ is 3.77× and 1.93× of FreeRider and MOXcatter when the original channel is blocked.

We firmly believe that RapidRider holds tremendous potential for various backscatter applications, offering a low-power, high-throughput communication solution by capitalizing on existing ambient signals. In this chapter, we put the tag data modulation granularity into the symbol-level. We will future discuss the sub-symbol Wi-Fi backscatter in the next chapter.

References

1. Liu V, Parks A, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. In: Proceedings of ACM SIGCOMM
2. Vasisht D, Zhang G, Abari O, Lu H, Flanz J, Katabi D (2018) Inbody backscatter communication and localization. In: Proceedings of ACM SIGCOMM
3. Hessar M, Najafi A, Gollakota S (2019) Netscatter: enabling large-scale backscatter networks. In: Proceedings of USENIX NSDI
4. Hu P, Zhang P, Rostami M, Ganesan D (2016) Braidio: an integrated active-passive radio for mobile devices with asymmetric energy budgets. In: Proceedings of ACM SIGCOMM
5. Wang J, Hassanieh H, Katabi D, Indyk P (2012) Efficient and reliable low-power backscatter networks. In: Proceedings of ACM SIGCOMM
6. Abari O, Vasisht D, Katabi D, Chandrakasan A (2015) Caraoke: an etoll transponder network for smart cities. In: Proceedings of ACM SIGCOMM
7. Iyer V, Nandakumar R, Wang A, Fuller SB, Gollakota S (2019) Living IoT: a flying wireless platform on live insects. In: Proceedings of ACM SIGCOMM
8. Zhang P, Ganesan D (2014) Enabling bit-by-bit backscatter communication in severe energy harvesting environments. In: Proceedings of USENIX NSDI
9. Hu P, Zhang P, Ganesan D (2015) Laissez-Faire: fully asymmetric backscatter communication. In: Proceedings of ACM SIGCOMM
10. Rostami M, Gummeson J, Kiaghadi A, Ganesan D (2018) Polymorphic radios: a new design paradigm for ultra-low power communication. In: Proceedings of ACM SIGCOMM
11. Gong W, Chen S, Liu J (2017) Towards higher throughput rate adaptation for backscatter networks. In: Proceedings of IEEE ICNP
12. Liu H, Gong W, Miao X, Liu K, He W (2014) Towards adaptive continuous scanning in large-scale RFID systems. In: Proceedings of IEEE INFOCOM
13. Liu H, Gong W, Chen L, He W, Liu K, Liu Y (2014) Generic composite counting in RFID systems. In: Proceedings of IEEE ICDCS
14. Gong W, Liu H, Liu K, Ma Q, Liu Y (2016) Exploiting channel diversity for rate adaptation in backscatter communication networks. In: Proceedings of IEEE INFOCOM
15. Gong W, Liu H, Liu J, Fan X, Liu K, Ma Q, Ji X (2018) Channelaware rate adaptation for backscatter networks. IEEE/ACM Trans Networking 26(2):751–764

16. Liu K, Ma Q, Gong W, Miao X, Liu Y (2014) Self-diagnosis for detecting system failures in large-scale wireless sensor networks. IEEE Trans Wirel Commun 13(10):5535–5545
17. Gong W, Stojmenovic I, Nayak A, Liu K, Liu H (2015) Fast and scalable counterfeits estimation for large-scale RFID systems. IEEE/ACM Trans Networking 24(2):1052–1064
18. Gong W, Liu J, Yang Z (2017) Efficient unknown tag detection in large-scale RFID systems with unreliable channels. IEEE/ACM Trans Networking 25(4):2528–2539
19. Gong W, Chen S, Liu J, Wang Z (2018) Mobirate: mobility-aware rate adaptation using PHY information for backscatter networks. In: Proceedings of IEEE INFOCOM
20. Gong W, Liu J, Yang Z (2016) Fast and reliable unknown tag detection in large-scale RFID systems. In: Proceedings of ACM MobiHoc
21. Wang A, Iyer V, Talla V, Smith JR, Gollakota S (2017) FM backscatter: enabling connected cities and smart fabrics. In: Proceedings of USENIX NSDI
22. Bharadia D, Joshi K, Kotaru M, Katti S (2015) Backfi: high throughput wifi backscatter. In: Proceedings of ACM SIGCOMM
23. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of ACM SIGCOMM
24. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of ACM SenSys
25. Ensworth JF, Reynolds MS (2017) BLE-backscatter: ultralow-power IoT nodes compatible with bluetooth 4.0 low energy (BLE) smartphones and tablets. IEEE Trans Microw Theory Tech 65(9):3360–3368
26. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of ACM CONEXT
27. Talla V, Hessar M, Kellogg B, Najafi A, Smith JR, Gollakota S (2017) LoRa backscatter: enabling the vision of ubiquitous connectivity. In: Proceedings of ACM IMWUT
28. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In: Proceedings of USENIX NSDI
29. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Intertechnology backscatter: towards internet connectivity for implanted devices. In: Proceedings of ACM SIGCOMM
30. Kellogg B, Parks A, Gollakota S, Smith JR, Wetherall D (2014) Wifi backscatter: Internet connectivity for RF-powered devices. In: Proceedings of ACM SIGCOMM
31. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of ACM MobiSys
32. Zhao J, Gong W, Liu J (2018) X-tandem: towards multi-hop backscatter communication with commodity wifi. In: Proceedings of ACM MobiCom
33. Wang Q, Chen S, Zhao J, Gong W (2021) Rapidrider: efficient wifi backscatter with uncontrolled ambient signals. In: Proceedings of IEEE INFOCOM

Chapter 5
Symbol and Sub-Symbol Wi-Fi Backscatter for 802.11b

Abstract Backscatter communication technology has garnered increasing attention as a solution to the high energy consumption resulting from the rapid growth of IoT devices. The IEEE 802.11b Wi-Fi protocol, proposed in 1999, remains compatible with most devices today. With the low power consumption and stable communication properties of backscatter technology, the 802.11b Wi-Fi signal has enormous potential in various fields, such as smart cities and communities. This chapter analyzes the characteristics of 802.11b Wi-Fi and backscatter communication systems and introduces two backscatter modulation methods based on 802.11b Wi-Fi signals. Regarding symbol level modulation, we present a single access point backscatter system that uses uncontrolled ambient signals and an efficient decoding algorithm based on DSSS Wi-Fi. Concerning sub-symbol level modulation, we introduce a CCK tag modulation method based on high-speed CCK Wi-Fi signals, which achieves higher throughput levels. We prototype our design using commodity Wi-Fi devices and FPGAs. Extensive experiments conducted on our prototype have demonstrated the effectiveness of our system. Our system can use different modulation methods to meet the demands of efficient communication based on environmental signals and high throughput support for video communication. We believe the proposed backscatter system is well-suited for emergency services in smart communities.

5.1 Introduction

Backscatter communication is a wireless communication technique that has received significant attention in recent years for its ability to enable cost-effective data transmission. It has been successfully applied in various wireless communication systems, including RFID, Bluetooth, and Wi-Fi. The IEEE 802.11b standard was introduced in 1999 to provide wireless connectivity at a maximum data rate of 11 Mbps. Although newer Wi-Fi standards offer faster data rates, 802.11b is still widely used in older devices that do not support newer standards. Due to the cost-effective nature of 802.11b Wi-Fi-based devices, it is an ideal option for smart homes

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_5

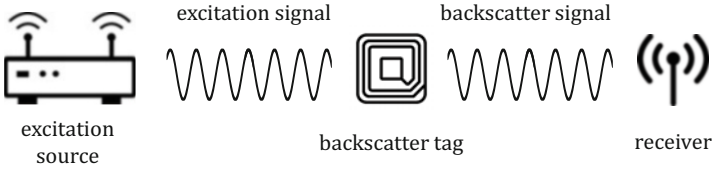


Fig. 5.1 The structure of typical backscatter system

and communities. Therefore, backscatter communication has a broad application prospect in 802.11b Wi-Fi networks.

A typical backscatter communication system comprises an excitation source, a backscatter tag, and a receiver shown in Fig. 5.1. The exciter generates excitation signals, which can be used to transmit continuous sine waves, predefined packets, or productive data. In addition, ambient backscatter systems can utilize existing ambient signals to enable communication between devices and power the system without using batteries [1, 2]. Backscatter tags can carry their data onto signals without demodulating excitation signals. In Wi-Fi-based backscatter systems, the backscatter tag selects the corresponding impedance according to the data to be transmitted, modifies the data segment of the backscatter packet, and moves the backscatter signal to a different channel from the excitation signal. In addition to demodulating the backscatter signal, the decoder at the receiver calculates the carried tag data according to the backscatter packet and the tag modulation method.

Backscatter communication offers several advantages over traditional wireless communication techniques. One of the primary benefits is its ability to operate over long distances without requiring a direct line of sight [3]. This advantage makes it an ideal technique for applications such as environmental monitoring, where devices may be placed in remote locations. Another advantage of backscatter communication is its low power consumption. Backscatter devices require very little power and can be designed to harvest energy from the environment [4]. When power consumption and working time are essential, backscatter technology can provide a communication system with a long working time and low power consumption. Emergency services such as first aid and security work in smart communities have high requirements for working time, energy consumption, and deployment cost [5, 6]. The backscatter communication system based on 802.11b Wi-Fi can perfectly meet complex requirements and play the role of efficient and low-power communication according to actual scenarios.

However, existing backscatter communication systems have several limitations. For instance, traditional backscatter systems require dedicated devices, which increases the deployment cost for large-scale applications. Due to the imprecise synchronization and high decoding complexity, current backscatter systems based on commercial devices and Wi-Fi signals mainly focus on symbol level modulation. To overcome the interference, FreeRider [7] modulates one tag bit on four Wi-Fi symbols, and SyncScatter [8] focuses on accurate synchronization to improve

the throughput. HitchHike [4] and SyncScatter [8] have a maximum throughput that does not exceed 1 Mbps, which limits the application scenarios of backscatter systems. The bandwidth requirement for high-definition video transmission is approximately 9 Mbps, and the systems mentioned above are inadequate to support video communication. The IEEE 802.11b protocol [9] provides complementary code keying (CCK) technology to support a data transmission rate of 11 Mbps, exceeding the threshold of 9 Mbps. Therefore, using CCK Wi-Fi signals to achieve high-throughput backscatter data transmission is a possible optimization direction to expand application scenarios. Yuan and Gong [10] offers an idea for high-throughput implementation based on CCK Wi-Fi signals.

Besides demodulating the backscatter signal to obtain the backscatter packet, another crucial point is to acquire the original data. A feasible solution is to have the excitation source send fixed packets. However, this method can lead to channel resource waste and interference with other regular communications. Alternatively, the receiver can receive and unpack the original excitation signal on another Wi-Fi channel. Nevertheless, the receiver with increased backscatter communication must attend to the excitation and backscatter signals, adding hardware requirements. Thus, obtaining the original packet based on the received backscatter packet can improve communication efficiency and reduce deployment costs.

Inspired by previous research, this chapter investigates the potential of backscatter technology as a low-cost, high-throughput solution for communications on 802.11b Wi-Fi signals. The main technical contributions are as follows:

For low-rate communication methods, such as 1 Mbps 802.11b Wi-Fi signals, a single Wi-Fi symbol corresponds to a single bit in the packet. We design a backscatter system based on symbol level modulation and CRC reverse decoding of ambient 802.11b Wi-Fi packets. This scheme utilizes ambient signals in the environment. In this backscatter communication system, tags carry data in the payload field by codeword translation. The receiver can decode the excitation packets from backscatter packets and obtain the tag data.

For high-rate communication methods, we use CCK modulation to transmit data over 802.11b Wi-Fi with a data transmission rate of 11 Mbps. Unlike OFDM, CCK focuses on the time domain, and each symbol contains eight bits. This facilitates sub-symbol modulation and improves backscatter throughput. We find that parallel phase items contain independent information that can be used for backscatter transmission. In sub-symbol level backscattering, the tag only modulates the PSDU field in the Wi-Fi packet. The tag transforms eight bits into phase shifts in eight time slots of a symbol and adds these phase shifts to the transmitted signals in corresponding time slots by toggling the RF switch. Finally, the tag modification can be extracted at the commodity receiver by reversing the scrambling and CCK-mapping operation.

In summary, this chapter proposes different modulation methods based on 802.11b Wi-Fi signals with different data rates. We use symbol level modulation for signals with low data rates to reduce hardware requirements and decode the original packet only from backscatter packets. We use sub-symbol level modulation for high data rate signals to increase the tag data transmission throughput. We discuss

the impact of error control codes on decoding accuracy and introduce the tradeoff between bit error rate (BER) and throughput. Compared to traditional backscatter systems based on 802.11b Wi-Fi signals, our system can meet different hardware and throughput requirements at different data rates. We build a prototype of our system using commodity Wi-Fi devices and FPGAs and evaluate its performance in different scenarios. The results demonstrate that our system achieves low BER and high throughput, and is suitable for high-definition video transmission.

5.2 Related Work

5.2.1 Backscattering with COTS Radios

The backscatter technology is first applied in RFID, and the platform WISP is designed for backscatter communication [11–13]. But these systems require dedicated devices in tag data transmission. To avoid dependence on dedicated hardware, ambient backscatter can utilize existing environmental signals as excitation signals to support tag communication [14]. Interscatter [15] proposes a modulation method for converting Bluetooth signals into Wi-Fi signals to support wireless communication in multi-protocol scenarios. Backscatter technology currently supported tag data transmission based on various wireless communication signals, including Wi-Fi [1–3, 16–18], Bluetooth [19–23], ZigBee [24–26], FM [27], etc. Due to the low energy consumption of backscatter technology and the low cost of commercial devices, backscatter communication systems have great potential applications in sensor networks [28–31], smart agriculture [32, 33] and other fields.

5.2.2 Codeword Translation

HitchHike [4] proposed a tag modulation technology named “codeword translation" based on 802.11b Wi-Fi signals. Syncscatter [8] focused on the synchronization problem and optimizes the backscatter system to achieve higher throughput. In addition, codeword translation has also been extended to Bluetooth [7], LoRa [34, 35], and other Wi-Fi protocols [36]. Our work follows the idea of codeword translation and pays attention to both low-speed and high-speed 802.11b Wi-Fi signals. We will introduce backscatter systems with different modulation granularity. The backscatter system based on CCK Wi-Fi and sub-symbol level modulation can achieve more than 10 Mbps of throughput, which has the prospect of application in a variety of practical environments.

5.2.3 *Smart Community*

The smart community is based on existing IoT devices to achieve efficient community management and a secure community environment [37]. In addition, smart communities can also combine advanced technologies such as artificial intelligence and cloud computing to improve risk perception and information processing efficiency [5, 38]. Similarly, the backscatter technology based on sensors and IoT devices in the environment can be applied to smart communities to solve the problems of high deployment costs and high energy consumption in the management, providing a promising prospect for large-scale deployment and promotion of smart communities [39, 40].

5.3 802.11b Wi-Fi Primer

5.3.1 *802.11b Wi-Fi Packet Format*

The 802.11b Wi-Fi packet is used for transmitting data over a wireless network, and it has a fixed packet structure, as shown in Fig. 5.2. The Wi-Fi packet includes PHY Preable, PHY Header, and PSDU. PHY Preable and PHY Header contain packet control information. When the receiver demodulates the backscatter signal, these packet control fields are significant for synchronization and decoding. PSDU contains a MAC frame, and the MAC frame has a header, payload, and CRC field. The payload contains transmitted data, and the CRC field is used for error detection. When the receiver finds that the received data and CRC value are not consistent, the receiver may abandon the received packet. The CRC verification function can be closed by opening the monitor mode in the Wi-Fi receiver hardware. In this way, the receiver can accept the 802.11b Wi-Fi packet with the wrong CRC checksum.

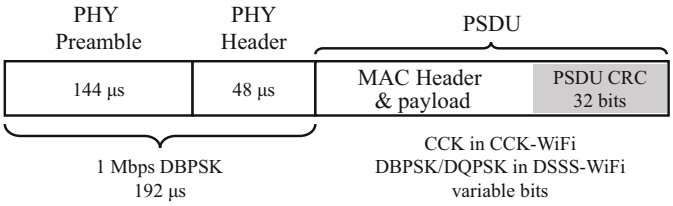


Fig. 5.2 802.11b Wi-Fi packet format

5.3.2 Low Rate DSSS Transmission

Low Rate Direct Sequence Spread Spectrum (DSSS) transmission is a method of transmitting data over a wireless network using a spread spectrum technique. For convenience, we refer to it as DSSS Wi-Fi. The technique involves spreading the signal over a wide frequency band, making it less susceptible to interference and more resistant to fading. This transmission type is typically used in low-power applications where long battery life is desired. In 802.11b Wi-Fi, Low Rate DSSS is used for 1 or 2 Mbps data rates. In this work, we focus on DSSS Wi-Fi signals with a speed of 1 Mbps. At 1 Mbps DSSS Wi-Fi, the modulation method for the transmitter is Differential Binary Phase Shift Keying (DBPSK). Traditional BPSK modulation uses two phases to encode bit 0 and 1, respectively. Instead of comparing the current phase of the carrier signal to a reference phase, as is done in traditional modulation, DBPSK compares the current phase to the phase of the previous symbol.

5.3.3 High Rate CCK Transmission

High Rate Complementary Code Keying transmission is another method of transmitting data over 802.11b Wi-Fi. For convenience, we refer to it as CCK Wi-Fi. CCK is used for higher data rates of up to 11 Mbps in 802.11b Wi-Fi. It uses a combination of complementary codes to increase the data transmission rate. CCK provides higher data rates by combining multiple bits into a single symbol, which is then transmitted over the wireless network. This technique allows for faster data transmission rates and is typically used in high-bandwidth applications. In this chapter, we focus on CCK Wi-Fi signals with a speed of 11 Mbps to achieve a high-speed tag data transmission. It should be noted that since the preamble and header contain important control information required for synchronization and demodulation, they cannot be modified by the backscatter tag.

5.4 Symbol Level Modulation Design

5.4.1 Overview

Wi-Fi signals transmit data using Wi-Fi symbols, modulated by DBPSK at a data rate of 1 Mbps according to the 802.11b packet format shown in Fig. 5.2. Backscatter systems based on symbol level modulation use ambient excitation signals carrying productive data in the environment, with the excitation data not controlled by the backscatter system. The tag uses codeword translation to encode tag data into the backscatter packet payload. The core challenge of our proposed system is to restore the original excitation packet from the backscatter packet since

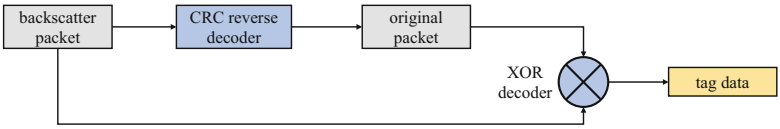


Fig. 5.3 The decoding procedure of symbol level modulation based backscatter system

the receiver can only receive and demodulate the backscatter signal. Since the tag only modifies the payload field in the DSSS Wi-Fi packet, the MAC Header and CRC value remain the same in the backscatter and original packets, and the modified data bits are unknown to the receiver. The CRC value is calculated via the MAC Header and original data using the CRC algorithm, meaning there is a functional constraint relationship between the MAC Header, original data, and CRC value. The proposed system uses CRC algorithms to calculate the original data from the available MAC header and CRC value. When the original excitation packet and backscatter packet are known, the system can decode the tag data using the efficient XOR decoder proposed in HitchHike [4]. The overview of the decoding procedure is shown in Fig. 5.3. This section will introduce the modulation method in the backscatter tag and the detailed decoding procedure in the receiver.

5.4.2 Codeword Translation and Symbol Level Modulation

HitchHike [4] introduced a novel tag modulation technique called codeword translation. In 1 Mbps DSSS Wi-Fi signals, two codewords are used to encode data bits, with a phase difference of 180° between them. By changing the codeword, backscatter tags can manipulate the data transmitted by backscatter signals. Specifically, for 1 Mbps DSSS Wi-Fi signals, the tag employs BPSK technology to append phase rotation on the backscatter signal based on transmitted tag data bits. When a transmitted tag data bit is 1, the backscatter tag adds a phase offset π on the corresponding Wi-Fi symbol, whereas it does not require phase rotation when the tag data bit is 0. The decoder at the receiver compares the difference between the original excitation packet and the received backscatter packet to obtain the position and phase information of the tag modulation, thereby decoding the tag data carried by the tag on the backscatter signal. This tag modulation uses the symbol level modulation method, where one tag data bit corresponds to one Wi-Fi symbol in the backscatter signal. According to the IEEE 802.11b protocol [9], each 1 Mbps DSSS Wi-Fi symbol corresponds to one data bit. Hence, in symbol level modulation, one tag data bit corresponds to one data bit in the backscatter packet.

5.4.3 CRC Reverse Decoding

In the DSSS Wi-Fi-based backscatter system, the backscatter tag utilizes the codeword translation technique to embed tag data into backscatter packets. The modulation starts from the first data bit of the payload and is continuous. The backscatter tag modifies the payload in the MAC frame while leaving the PSDU CRC field unchanged. While the receiver can obtain a backscatter packet through the standard demodulation process, the original excitation packet needs to be obtained using known backscatter packets and tag modulation algorithms. Our designed decoder can utilize the functional relationship between the PSDU CRC field and payload to compute the original data based on known CRC values.

5.4.3.1 CRC Algorithms

We first introduce the bit-oriented algorithm related to CRC value calculation, which can be summarized as Algorithm 1. The transmitter uses a CRC register to compute the CRC value based on known data bits through operations such as bit-shift and XOR. The length of the CRC sequence in PSDU is 32 bits, so the length of the CRC register is 32 bits. The CRC algorithm includes three constants: CRCPOLY, INITXOR, and FINALXOR. The values of the constants in CRC are CRCPOLY=0x04C11DB7, INITXOR=FINALXOR=0xFFFFFFFF. When calculating the CRC registers, we can use the initial and final states of the CRC register instead of INITXOR and FINALXOR. For instance, if the initial register value r' of the CRC is known, INITXOR needs to be replaced with r', and the CRC register value computed through the while loop is the final value r.

Algorithm 1 CRC calculation algorithm

Input: data bits a
Output: CRC register value $crcreg$
  $crcreg \leftarrow$ INITXOR
  $i \leftarrow 0$
  while $i < a.length$ **do**
    LEFTSHIFT($crcreg$)
    if $bit\_just\_shifted\_out \neq a_i$ **then**
      $crcreg \leftarrow crcreg \oplus$ CRCPOLY
    end if
    $i \leftarrow i + 1$
  end while
  $crcreg \leftarrow crcreg \oplus$ FINALXOR

Algorithm 2 CRC reverse calculation algorithm

Input: final CRC register value r, reversed data bits a
Output: initial CRC register value r'

```
i ← a.length − 1
crcreg ← r
while i ≥ 0 do
  if crcreg_31 = 1 then
    crcreg ← crcreg ⊕ CRCPOLY
    RIGHTSHIFT(crcreg)
    crcreg_0 = a_i ⊕ 1
  else
    RIGHTSHIFT(crcreg)
    crcreg_0 = a_i
  end if
  i ← i − 1
end while
r' ← crcreg
```

Algorithm 2 shows the bit-oriented CRC reverse algorithm, which is used to find the initial value r' of the register when the data bit a and the final value r of the register are known. There is a functional relationship between the initial value r' of the CRC register, the final state value r of the CRC register, and the data bit a in the two CRC algorithms. The average time complexity of the CRC algorithm operation is related to the data bit length. To simplify the representation, we use Eq. 5.1 to indicate the functions corresponding to the two CRC algorithms.

$$r = crc(r', a), \quad r' = crc\_reverse(r, a). \tag{5.1}$$

5.4.3.2 CRC Reverse Problem

The CRC algorithm calculates the CRC register value based on the data bits in a forward or backward manner. However, the problem arises when determining the unknown data bits from the known initial and final states of the registers. If the unknown data length is denoted by l, [41] shows that the number of possible data bit sequence solutions is 2^{l-32} when l is greater than 32 bits, while it is unique when l is less than or equal to 32 bits. We can use the following function to represent the relationship between the length of data bits l and the number of solutions N_l. Therefore, to ensure the uniqueness of the results and improve data transmission efficiency, we discuss the case where the data length is set to 32 bits.

$$N_l = \begin{cases} 2^{l-32}, & l > 32 \\ 1, & l \leq 32 \end{cases} \tag{5.2}$$

In both CRC algorithms, the data sequence a is the independent variable of the function. Since the CRC reverse problem requires calculating the unknown data

sequence with known CRC register values, we need to derive a function based on the existing functional relationships between the independent variable of the register value and the dependent variable of the data sequence. Stigge et al. [41] provides an equation that describes this functional relationship based on the properties of the CRC algorithm shown in Eq. 5.3.

$$crc(r', a) = crc(a, r') = r. \tag{5.3}$$

Combining the correlation equations leads to Eq. 5.4 for calculating data bits based on CRC register values. It is important to note that the establishment of this equation requires the data bits a to be of 32-bit length.

$$a = crc\_reverse(r, r'). \tag{5.4}$$

5.4.3.3 Calculation of Original Data

The main challenge in the receiver decoding procedure is to determine the unknown original data from known MAC headers and CRC values. While brute force search could theoretically find the unknown data, the number of enumeration sequences grows exponentially with the length of the original data, rendering it impractical to use enumeration methods to obtain the original data. Section 5.4.3.2 introduces an effective method for calculating original data based on CRC register values. As outlined in Eq. 5.4, the decoder needs to calculate the initial and final values of the CRC register before determining the unknown data bits. The CRC register's initial value can be computed using the unmodified MAC header and CRC algorithm. By applying XOR operations to the unmodified received CRC values and FINALXOR, the decoder can obtain the final value of the CRC register. The decoder can then compute the original data using Eq. 5.4. Algorithm 3 outlines the process by which the decoder decodes the original data bits based on the backscatter packet. The original excitation packet can be obtained by substituting the data sequence in the backscatter packet with the calculated original data.

Algorithm 3 Calculation in CRC reverse decoder

Input: MAC header K, CRC32 sequence R
Output: original data a
$r \leftarrow R \oplus$ FINALXOR
$r' \leftarrow crc$(INITXOR, K)
$a \leftarrow crc\_reverse(r, r')$

Given that the original data length is 32 bits and the backscatter tag employs symbol level modulation, the tag data length cannot exceed 32 bits. As the entire original data sequence must be restored during decoding, the average runtime of the reverse algorithm for restoring the original data is unrelated to the tag data length.

5.4.3.4 Calculation of Tag Data

As the backscatter tag uses codeword translation to modulate tag data, and the decoder can obtain the original packet via Algorithm 3, the backscatter system can use an effective XOR decoder presented by HitchHike [4] to compute the tag data from the backscatter packet and original packet.

5.4.3.5 Extension of Encoding Method

The backscatter tag's symbol level modulation method continuously modulates 32 bits, allowing the system to employ complex tag data encoding algorithms. This section introduces two feasible and advanced encoding methods for backscatter tags.

The first encoding method is the sliding window method. The previous tag adds a phase offset to the corresponding position of the backscatter packet based on the transmitted tag data. When excitation data is long, the continuous modulation method fails to use the abundant modulation space in Wi-Fi packets. To overcome this, we can divide the tag data into two segments. One part serves as modulation data information, and the tag calculates the corresponding phase rotation based on the codeword translation method. The other part serves as modulation position information, and the tag calculates the starting position of modulation based on the bit sequence and loads the other part of the modulation data into the backscatter packet. Thus, the modulation position and data are determined by the tag data from the backscatter packet modulation perspective.

The second encoding method is the redundant check bit method. The PSDU CRC has error detection functions to protect data within the PSDU. Due to the absence of check code in the tag data, noise interference will result in more bit errors in decoding results. To enhance decoding accuracy, we can use error control codes such as error detecting codes like parity bits and forward error correction (FEC) codes like Hamming codes, as shown in Fig. 5.4.

For parity codes, tags need to calculate the sequence of parity codes based on real tag data and append them to the end of the tag data. Furthermore, the receiver needs to perform additional error detection after decoding the tag data. If the decoded tag data and checksum are inconsistent, the receiver discards the incorrect calculation result, thereby preserving the decoded tag data with higher accuracy. For Hamming codes, the backscatter tag segment long tag data and add

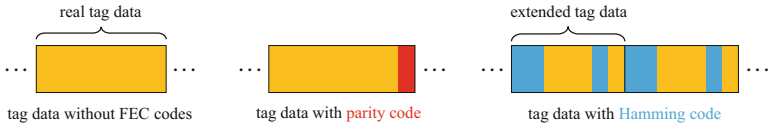


Fig. 5.4 Different error control codes

redundant check bits. Since Hamming code offers error detection and correction functions, the decoder can correct the error decoding result following the error correction algorithm of Hamming code when the decoding outcome is incorrect. FEC codes can significantly resolve the problem of sudden bit errors resulting from noise interference when fewer bit errors exist.

Nevertheless, adding redundant bits may lower the system's effective throughput, and the verification process may impact the data transmission performance of the system when the error correction code's complexity is high. Therefore, system designers must choose the optimal error control code based on throughput and accuracy requirements for real-world scenarios.

5.5 Sub-Symbol Level Modulation Design

5.5.1 Overview

Due to the inability of low-speed 802.11b Wi-Fi signals to meet the high throughput requirements such as video communication, high-speed Wi-Fi signals based on CCK technology have been proposed. The process of transmitting and receiving CCK Wi-Fi signals is depicted in Fig. 5.5. The transmitted data undergoes scrambling and is then mapped to four parallel phase items through CCK mapping at the transmitter. The Wi-Fi symbol is transmitted using eight time slots with distinct phases. This encoding technique allows the transmitter to convey multiple data bits within a single Wi-Fi symbol, achieving a maximum throughput of 11 Mbps. Noise interference and tag modulation can affect the transmitted data during signal transmission. At the receiver, a reverse procedure is employed, which involves descrambling and CCK demapping to retrieve the backscatter packet.

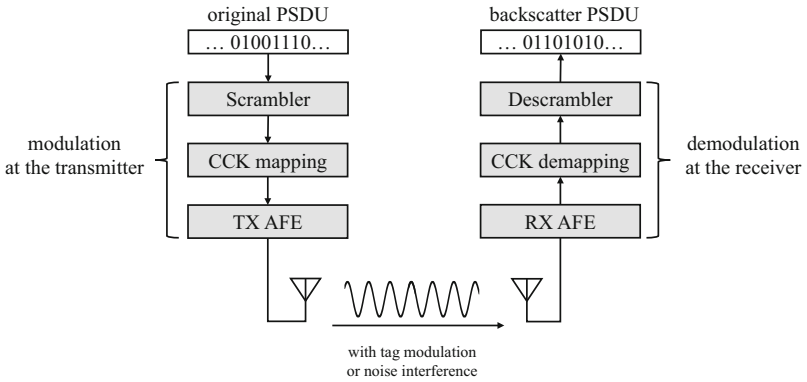


Fig. 5.5 The transmitting and receiving procedure of CCK Wi-Fi signal

The 11 Mbps CCK Wi-Fi symbol differs from the 1 Mbps DSSS Wi-Fi signal because it contains multiple bits in the PSDU. Specifically, at a data rate of 11 Mbps, a Wi-Fi symbol can transmit eight data bits. The tag associated with the symbol level modification alters several data bits within the Wi-Fi packet through phase rotation across the entire Wi-Fi symbol, resulting in multiple backscatter bits corresponding to one tag data bit. The CCK Wi-Fi-based backscatter system requires a more sophisticated modulation method to attain the maximum tag data transmission rate. This section introduces the parallel transmission property of CCK Wi-Fi and the sub-symbol level modulation employed by the backscatter tag. Furthermore, to extend the system's application range and improve decoding accuracy, we also discuss the extension of parallelism transmission and the synchronization requirement.

5.5.2 Sub-Symbol Modulation

5.5.2.1 Parallel Transmission and Sub-Symbol Modulation

The key to achieving high-speed data transmission lies in CCK technology. We provide an overview of parallel transmission from the perspective of the transmitter. According to Fig. 5.5, the transmitted data is scrambled and divided into octets, and we represent it as $a = [a_0, a_1, a_2, \ldots, a_7]^{\mathrm{T}}$. Each octet is mapped to a corresponding phase, denoted as $\phi = [\phi_1, \phi_2, \phi_3, \phi_4]^{\mathrm{T}}$. Specifically, the transmitter utilizes DQPSK technology to encode the bit pair a_0a_1 as ϕ_1. Similarly, a_2a_3, a_4a_5, and a_6a_7 are respectively mapped to ϕ_2, ϕ_3, and ϕ_4 using QPSK technology. We can consider the process of the four phases ϕ_1, ϕ_2, ϕ_3, and ϕ_4 as four parallel transmissions, each phase carrying its corresponding data. Within an 802.11b CCK Wi-Fi symbol, there are eight equally long time slots, represented as $\psi = [\psi_0, \psi_1, \psi_2, \ldots, \psi_7]^{\mathrm{T}}$, each associated with a specific phase. The 802.11b protocol defines the correspondence between ψ and ϕ, as shown in the following formula.

$$\begin{gathered} \psi = A\phi + r \\ A^{\mathrm{T}} = \begin{pmatrix} 1\,1\,1\,1\,1\,1\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1\,0 \\ 1\,1\,0\,0\,1\,1\,0\,0 \\ 1\,1\,1\,1\,0\,0\,0\,0 \end{pmatrix} \\ r^{\mathrm{T}} = \begin{pmatrix} 0\,0\,0\,\pi\,0\,0\,\pi\,0 \end{pmatrix} \end{gathered} \tag{5.5}$$

Equation 5.5 utilizes matrix A to represent the transformation matrix, whereas matrix r represents an additional phase. We observe that phase ϕ_1 impacts every time slot, while ψ_3 and ψ_6 exhibit a phase increase of π compared to other parameters. The relationship between data bits and phase ϕ, as well as ϕ and ψ,

enables the transmitter to generate the waveform based on the transmitted data bits. Regarding the receiver, phase ϕ can be calculated based on phase ψ using the reverse process described in Eq. 5.6. This calculation allows for obtaining the backscatter packet data based on the received backscatter signal.

$$\phi = (A^{\mathrm{T}}A)A^{\mathrm{T}}(\psi - r) \tag{5.6}$$

For the backscatter tag, tag modulation involves modifying the phase of ψ. However, if the tag adds an extra phase in a single time slot, it may lead to incorrect decoding results at the receiver. Therefore, the modulation method must ensure that it does not impact the reception and decoding process, maintaining the backscatter signal as an effective Wi-Fi signal.

Inspired by the CCK mapping process, we have devised a sub-symbol level modulation method. This method enables the tag to calculate the phase increase at each time slot based on the transmitted data, thereby achieving tag data transmission. The tag employs a coding method similar to CCK mapping in phase modulation. Firstly, the tag divides the tag data into multiple octets, represented as $t = [t_0, t_1, t_2, \ldots, t_7]^{\mathrm{T}}$, which corresponds to eight tag data bits from a single octet. Then, using QPSK technology, the tag maps tag data octet t to $\phi_T = [\phi_{T_1}, \phi_{T_2}, \phi_{T_3}, \phi_{T_4}]^{\mathrm{T}}$ and utilizes matrix A in Eq. 5.5 to convert ϕ_T into phase rotation ψ_T in each time slot. Figure 5.6 displays a CCK Wi-Fi symbol in the backscatter signal after the sub-symbol level modulation. Regarding the receiver, the phase of the received signal can be expressed using the composition of the modulation phase by transmitter and tag, demonstrating that it can be correctly received and decoded.

Given that the receiving end possesses prior knowledge of the predefined excitation packet and the modified backscatter packet, the decoding process of tag

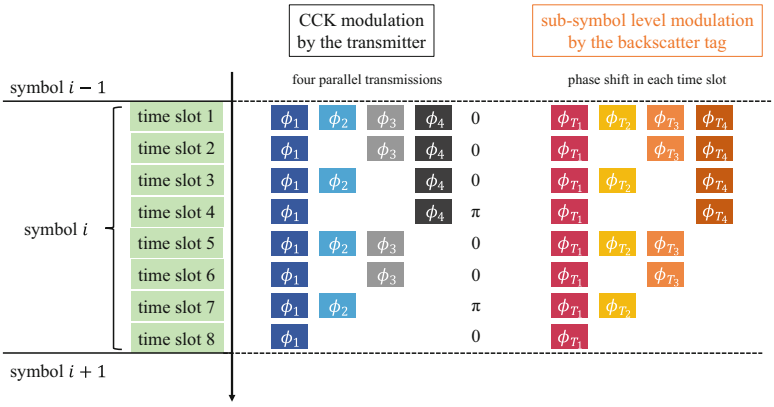


Fig. 5.6 The phase of the backscatter signal of a CCK Wi-Fi symbol in sub-symbol level modulation

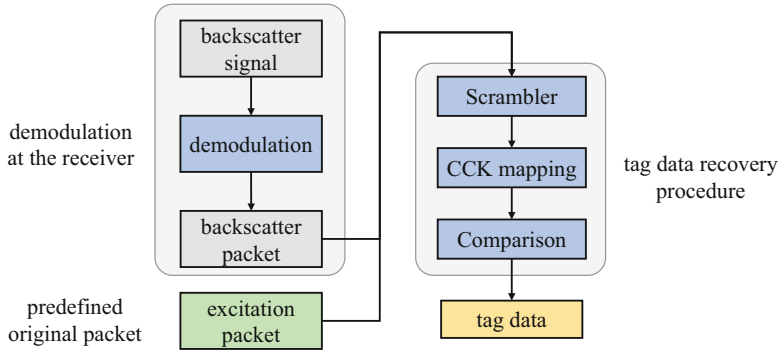


Fig. 5.7 The decoding procedure of sub-symbol level modulation at the receiver

data involves restoring the phase rotation introduced to the Wi-Fi signal by the tag. To accomplish tag data decoding, the receiver follows the steps depicted in Fig. 5.7. Initially, the decoder employs scrambling and CCK mapping procedures to retrieve the excitation and backscatter signals. Subsequently, the decoder compares the tag modulation in the Wi-Fi signal and deduces the transmitted tag data based on the modulation position and phase difference.

The sub-symbol level modulation method we have devised leverages all four parallel transmissions during the tag data modulation process. Due to the similarity in modulation methods between the tag and the transmitter, a theoretical maximum transmission rate of 11 Mbps can be achieved for tag data. Furthermore, the tag's capability to modify backscatter data at the sub-symbol level makes optimizing the traditional practice of turning off CRC verification at the receiver possible. The tag can calculate the modified transmission data by utilizing the available excitation packet and tag data, facilitating the calculation of the CRC field value within the backscatter packet. Then, the tag employs a similar sub-symbol level modulation method to modify the CRC value in the CCK Wi-Fi packet, enabling successful CRC verification at the receiver. To mitigate noise interference and enhance decoding accuracy, tags can also employ FEC codes introduced in Sect. 5.4.3.5 to safeguard tag data, including Hamming codes. The redundant check bits may reduce the efficiency of effective tag data transmission. Thus, the appropriate FEC code should be selected based on the specific scenario when deploying the backscatter communication system.

In conclusion, the sub-symbol level modulation-based backscatter system achieves high-speed tag data transmission while ensuring compliance with the regulations outlined in the IEEE 802.11b protocol. The tag data transmission can be protected using FEC codes, thereby improving decoding accuracy.

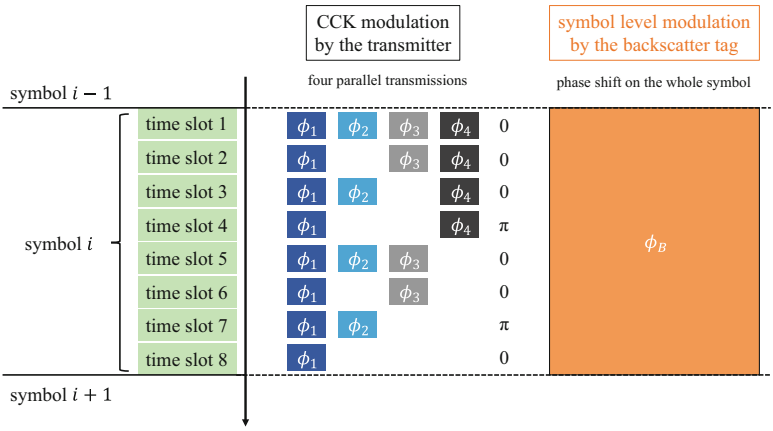


Fig. 5.8 The phase of the backscatter signal of a CCK Wi-Fi symbol in symbol level modulation

5.5.2.2 Comparison with Symbol Level Modulation

Apart from the sub-symbol level modulation method based on CCK, backscatter tags can also use symbol level modulation with CCK Wi-Fi. HitchHike introduced the codeword translation technique, which allows the backscatter tag to piggyback tag data by phase rotations of CCK Wi-Fi symbols. In contrast to sub-symbol level modulation, the minimum modulation unit for symbol level modulation is a CCK Wi-Fi symbol. The tag is required to encode tag data using QPSK and add a phase offset to the corresponding CCK Wi-Fi symbol. For the sake of discussion, we assume that the phase rotation is ϕ_B.

Figure 5.8 illustrates the phase rotation in tag modulation. We observe that symbol level modulation can be seen as a particular case of sub-symbol level modulation. Due to the same impact on every time slot in the CCK Wi-Fi symbol, the phase offset ϕ_B can be regarded as added to the ϕ_1, which means the backscattered phase $\phi' = [(\phi_1 + \phi_B), \phi_2, \phi_3, \phi_4]^{\mathrm{T}}$. Based on the observation and the nature of parallel transmission, we speculate that the maximum value of symbol level modulation throughput is 1/4 of the maximum value of sub-symbol level modulation throughput since the backscatter tag uses only one of the four phases to carry tag data. Moreover, since one CCK Wi-Fi symbol corresponds to multiple data bits, it is challenging for the backscatter tag to modify the CRC value of the backscatter packet. To prevent the backscatter packet from being discarded due to failure to pass the PSDU CRC verification, we must disable the CRC check step at the receiver.

5.5.2.3 Extension of Parallel Transmission

We have introduced that CCK Wi-Fi employs four independent parallel transmissions. When fully utilizing these four phase items, the maximum tag data transmission rate can reach 11 Mbps. Based on the parallel transmission, we propose several possible expansion plans further to improve the performance of the backscatter communication system.

One possible design to increase the tag data transmission rate is to increase the number of phase items in data transmission. In a 4-way parallel communication system, the backscatter tag can piggyback tag data on 16 phase items. Based on the property of parallelism, we can deduce that the maximum throughput of this backscatter system can reach 44 Mbps. With the improvement of communication throughput, the quality and efficiency of video transmission will be further improved, making it easier to apply in areas with higher performance requirements, such as city security and fire protection.

Another possible solution is to use distributed devices to decode tag data. In addition to the regular reception and demodulation time of the backscatter packet at the receiver, the decoding time of the tag data by the decoder based on the backscatter packet and predefined data cannot be ignored. As the length of tag data increases, a single decoder must process more information, leading to significant delays in data reception and decoding. The parallel transmission feature in CCK Wi-Fi allows decoding tag data using a distributed scheme. For existing modulation methods, the receiver can deploy four parallel decoders, each responsible for decoding a single phase item. Compared to calculating the entire tag data using a single decoder, parallel methods can significantly reduce the receiver's decoding time.

In summary, based on the parallelism of CCK Wi-Fi, we discussed possible expansion schemes of existing backscatter systems in parallel transmission and parallel decoding. However, the new designs require sophisticated signal processing algorithms and hardware, which can be expensive and complex to implement and should be carefully considered.

5.5.2.4 Synchronization Requirement

In sub-symbol level modulation, the backscatter tag has a crucial role. It identifies the excitation packet, locates the payload field's starting position in the Wi-Fi packet, and accurately loads the correct phase modulation into the appropriate time slot. Failing to achieve accurate synchronization can result in incorrect decoding, invalid data packets, and the inability to be received by the receiver. Previous backscatter systems employ larger modulation granularity or redundancy to enhance fault tolerance. For instance, FreeRider used four excitation symbols to carry one tag bit, while SyncScatter improved the synchronization accuracy. In contrast, our proposed sub-symbol level modulation uses one Wi-Fi symbol to carry multiple tag bits. Compared to DSSS Wi-Fi-based backscatter systems that use redundant

methods, sub-symbol level modulation has a more significant impact on the results when facing the same synchronization error. Therefore, precise control of sub-symbol level synchronization is necessary.

Traditionally, the synchronization method involves a simple signal energy detection method. The system uses an envelope detector and a comparator at the tag that provides a rising edge in the comparator output when the excitation signal arrives, indicating the beginning of a packet. However, the excitation signal has a power-on ramp at the start of a packet that has a duration of no more than two μs but is significant and cannot be ignored. Simply relying on the rising edge can easily cause synchronization deviation, leading to an offset in the modulation start time slot, which may ruin the control information and result in illegal Wi-Fi packets. Additionally, the specific power ramp duration is unregulated and may drift with time, resulting in additional errors when detecting the rising power for synchronization. Therefore, this rough method has considerable synchronization errors.

Due to the predefined packets and signals sent by the CCK Wi-Fi transmitter, a possible precise synchronization method is to compare packet header information. Unlike simple energy detection, the backscatter tag needs to monitor the signal strength over time and export binary sequences. By comparing the features with predefined signals using a comparator, the backscatter tag can better find the excitation signal and the starting position of the excitation packet. The parameters for similarity measurement can be set to Hamming distance, high-level frequency, etc. This method has a higher circuit complexity than rough synchronization, but using a comparator for bit comparison is still acceptable for tags.

Although precise synchronization circuits and algorithms may introduce additional computational and communication delays, we believe that the benefits of sub-symbol level modulation in high throughput and efficient communication outweigh the extra overhead. In summary, controlling synchronization errors is necessary from a theoretical perspective. Only more accurate synchronization can enable our carefully designed CCK modulation method to accurately align tag modulation to excitation symbols and add tag phases into the excitation at precise time slots.

5.6 Performance Evaluation

5.6.1 Implementation

We have introduced the design of a high-throughput system that takes advantage of the parallel transmission characteristics of CCK Wi-Fi and the tag modulation method based on sub-symbol level modulation. In this section, we build a prototype using commercial devices and evaluate the effectiveness and performance of the proposed backscatter system. The overview of the system prototype is shown in

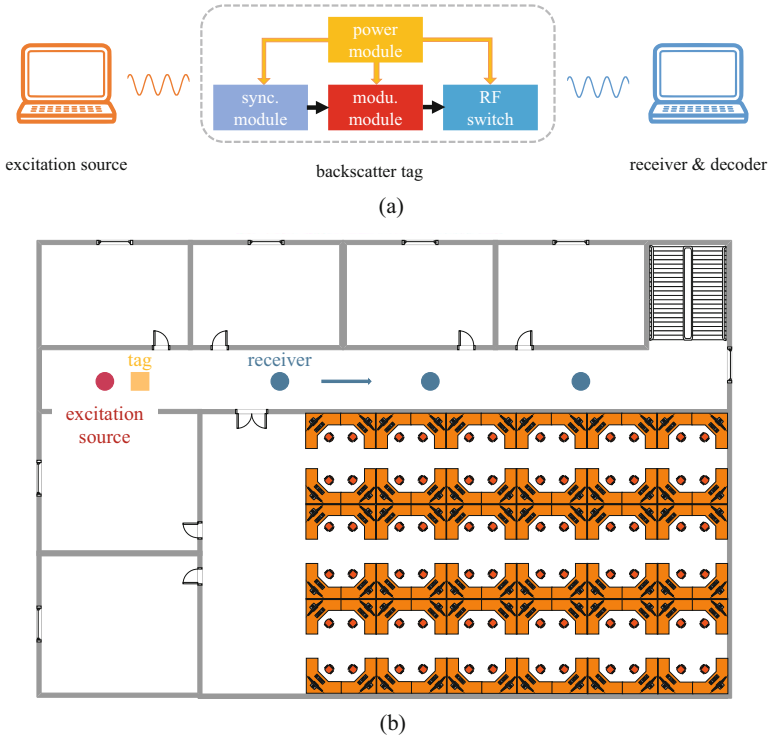


Fig. 5.9 The prototype and experiment scenario of the sub-symbol backscatter system. (**a**) The system overview. (**b**) Experiment scenario

Fig. 5.9. To verify the system's performance in a real-world environment, we set up two scenarios in the office area corridor. In the line of sight (LOS) scenario, there are no obstacles between the transmitter, tag, and receiver, while in the non line of sight (NLOS) scenario, a wooden board acts as an obstacle between the tag and the receiver. The transmitter utilizes a power amplifier to increase the power to approximately 20 dBm, and a 3 dBi glue stick antenna is employed. We introduce the specific components of the backscatter system in the following subsections.

5.6.1.1 Transmitter and Receiver

We use two laptops equipped with Qualcomm Atheros AR938X NICs, one as the transmitter and the other as the receiver. The transmitter is controlled by CommView for Wi-Fi software, which allows us to control the content of the excitation packet, while the receiver can capture the packet and decode the backscatter data from CCK Wi-Fi signals. Both the transmitted and received packets are legal 11 Mbps CCK

Wi-Fi packets without any additional requirements. The receiver should verify the CRC value of the backscatter PSDU during the receiving process.

5.6.1.2 Backscatter Tag

Synchronization Module The synchronization module facilitates the synchronization of the excitation signals. This module uses an envelope detector to identify the excitation packet through the comparator output's rising edge. To achieve more precise synchronization, the synchronization circuit can extract a binary sequence from the excitation signal and compare it with predefined sequences. The backscatter tag can achieve synchronization based on the similarity of the comparison results. This method results in more accurate synchronization than the energy detection approach. The synchronization module comprises capacitors, resistors, and inductors, as well as a 3dBi-glue-stick antenna, two Avago HSMS-2862 diodes, and an ON Semiconductor NCS2250 comparator.

Modulation Module The modulation module is responsible for the control of the backscatter tag. This module calculates the sub-symbol modulation parameters based on tag data and controls the RF switch to perform tag modulation. To transmit the tag data bits and ensure the legality of the backscatter packet, the modulation module also computes the PSDU CRC value of the backscatter packet via a predefined excitation packet and transmitted tag data. Based on the sub-symbol level modulation method and the above calculation results, the tag can determine the phase shift of the corresponding time slot in each modulated 802.11b CCK Wi-Fi symbol. Finally, the modulation module controls the RF switch to achieve the frequency and phase shift, thereby accomplishing the sub-symbol modulation and backscatter of the signal. These calculation and control functions are implemented in a Microchip AGLN250 low-power FPGA.

RF Switch The Analog ADG902 single-pole single-throw (SPST) RF switch is the core component of the backscatter tag. The RF switch adds an additional phase to the excitation signal based on the modulation module's calculated results for each time slot of the CCK Wi-Fi signal. The modulation module uses a finite state machine for QPSK modulation, which selects the impedance state corresponding to the phase shift for the RF switch to realize different phase shifts in tag modulation. In addition, the RF switch can use a square wave with a frequency of Δf to make the backscatter signal have a frequency offset Δf compared with the original excitation signal. This frequency shift ensures that the backscatter and excitation signals are in non-overlapping channels, thus reducing the interference between signals and improving the receiving accuracy.

Power Module The backscatter system's power module has energy management and storage functions to obtain communication energy from the surrounding environment without using a power supply. The sharing management chip TI BQ25570 and a 1000 μF capacitor for energy storage are used in the experiment.

In practical use, the control module converts the power supply mode to charging mode when the voltage of the capacitor is lower than the operating voltage of the device. After obtaining sufficient energy, the capacitor switches from charging to discharging, providing a power supply for synchronization, modulation, and other functions in the backscatter tag. The backscatter system communicates periodically during the switching cycle of the two modes. This green energy harvesting method can overcome traditional battery replacement shortcomings and conventional power sources' limitations on usage scenarios in large-scale applications.

5.6.1.3 Other Devices and Total Cost

Apart from the four core components of the backscatter tag, an Analog LTC6930 oscillator drives the FPGA, and the TI TPS73615 provides the 1.5 V power rail for the FPGA core. As the system is based entirely on commercial equipment, the critical components for the tag are easily obtainable. The total cost of the tag prototypes, including various critical equipment and necessary capacitors, resistors, and inductors, is estimated to be at most $50. The off-the-shelf device and acceptable price make the system's deployment more convenient.

5.6.2 Evaluation

5.6.2.1 Parallel Transmission Verification

We have explained that CCK Wi-Fi uses four parallel transmissions for high-speed data transmission, and its throughput is sufficient for high-definition video communication. To verify the isolation between parallel transmissions, we modulated one phase in each parallel transmission while keeping the others unmodified using the backscatter tag. Specifically, we modulated the phases of ϕ_1, ϕ_2, ϕ_3, and ϕ_4, respectively. At the receiver, we observed the recovery results of demodulating backscatter signals and verified the consistency between modulation and demodulation.

Figure 5.10 presents the tag data recovery result. We observe that the recovery results for all four phases have an accuracy exceeding 99.5%, and the average error rate is less than 1%, indicating the parallelism of the four phases in data

Fig. 5.10 The verification of the isolation between phase items in sub-symbol backscatter modulation

		Demodulation			
		ϕ_1	ϕ_2	ϕ_3	ϕ_4
Modulation	ϕ_1	0.999	0.004	0.003	0.002
	ϕ_2	0	0.996	0.002	0.001
	ϕ_3	0.001	0.005	0.997	0.002
	ϕ_4	0	0.002	0.002	0.999

transmission. We also notice that when only one phase is modulated, the sum of the demodulated phase ratios is not equal to 1. For example, when modulating ϕ_3, 0.3%+0.2%+99.7%+0.2%≠1. That's because this is not a classification or identification problem, four phase items are processed and recovered separately. The reason for this error is the occasional leakage between phase items, and it doesn't have a serious impact on the parallelism of transmissions.

In summary, the isolation between parallel transmissions is good enough for the tag to use all of them concurrently. The throughput of tag data transmission is linearly related to the phase number of modulation. The verified parallelism further demonstrates that in CCK Wi-Fi, the throughput of symbol level modulation is one-fourth that of sub-symbol level modulation. To achieve the highest throughput, the tag needs to use our designed modulation method to modulate four phases simultaneously. Therefore, we generate four parallel backscatter transmissions using one CCK Wi-Fi stream in tag modulation.

5.6.2.2 End-to-End Performance

In the sub-symbol backscatter system, the predefined CCK Wi-Fi packets are sent by the transmitter, meaning that the tag and receiver are both aware of the transmitted data in the excitation packet. We set the distance between the tag and the transmitter to 20 cm. To achieve sub-symbol modulation, the tag uses synchronization, modulation, and other modules to carry tag data on the backscatter PSDU. The tag is required to calculate the CRC of the backscatter packet based on the original packet and the modulated tag data, and make modifications to ensure the effectiveness of the Wi-Fi packet. The receiver can perform regular unpacking and CRC verification on backscatter signals received by the laptop's embedded antenna using CommView for Wi-Fi software. Then, the receiver restores the tag modulation's phase information based on the original packet and the modified backscatter packet to obtain the tag data. To test the system's optimal performance, the tag modulates all four parallel transmissions, and additional power is supplied to keep the system operational. In the experiment, we vary the distance between the receiver and the tag and assess its impact on critical performances such as system throughput and decoding accuracy.

The experimental results are presented in Fig. 5.11. The maximum tag data throughput is achieved when the distance between the backscatter tag and receiver is 2 meters, reaching around 10.8 Mbps. The maximum communication distance for LOS deployment is 20 m, while the maximum working distance for NLOS deployment is 18 m. The system's average throughput within the working distance range is higher than the threshold required for high-definition video communication. The high throughput is suitable for real-time high-definition video transmission in indoor environments or communities. The system's high decoding accuracy is also maintained while ensuring throughput. Figure 5.11 shows that at a distance of 2 m, the BER is below 1%, and the packet error rate (PER) is around 10%. When the communication distance is within 10 m, the BER is below 2.5%, and

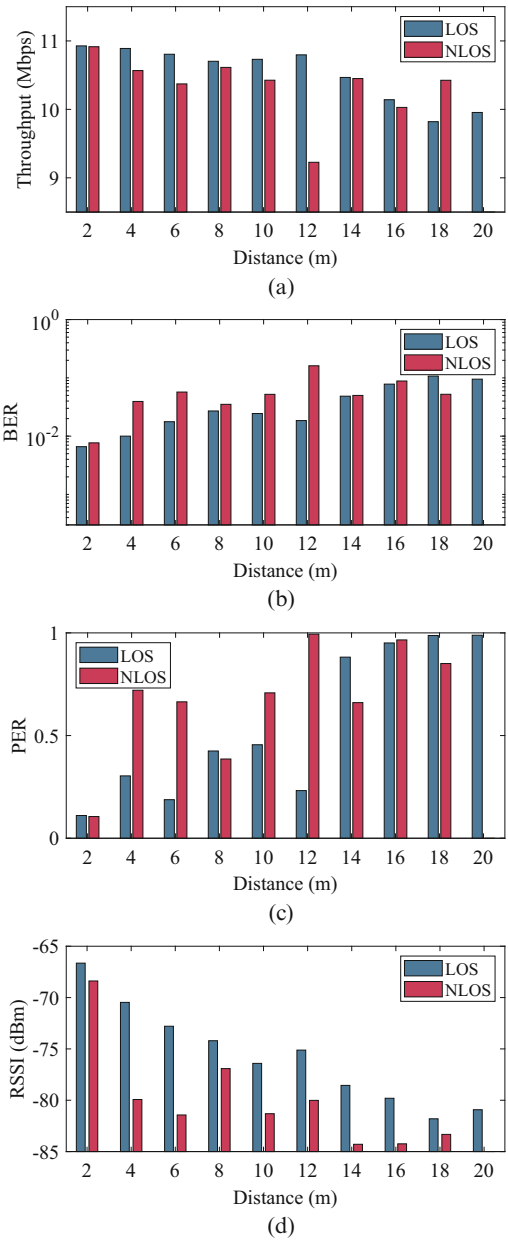


Fig. 5.11 Backscatter throughput, BER, PER and RSSI performance in LOS and NLOS deployments. (**a**) Throughput. (**b**) BER. (**c**) PER. (**d**) RSSI

the PER is less than 50%. At the maximum distance, the BER is approximately 10%, and the PER is close to 100%. The curve indicates that the BER and PER significantly increase as the communication distance increases. Since backscatter signals are more prone to noise and interference, backscatter packets derived by the

receiver contain more error bits as the distance increases, leading to errors in the corresponding decoded tag data. Particularly in NLOS scenarios, obstacles reflect a considerable part of backscatter signals, making it more difficult for the receiver to complete the reception and demodulation of backscatter packets. Therefore, the system performance in the LOS scenario is superior to that in the NLOS scenario. To quantitatively analyze the impact of distance on signal energy, we use the received signal strength indicator (RSSI) as an indicator in the experiment. The signal strength at the receiver decreases as the distance increases, which is confirmed by the RSSI curve displayed in Fig. 5.11. We observe that the average signal strength is weaker in the NLOS scenario than in the LOS scenario. In practical applications, obstacles in the environment, including trees and pedestrians, can impact the communication distance and data transmission efficiency of the backscatter system. Longer distance high-speed data transmission requires improving system hardware performances. Our future work will explore the relationship between obstacle types and performance.

We compare our system's performance with that of two other backscatter systems based on 802.11b Wi-Fi and commercial devices, HitchHike and SyncScatter. For the convenience of analysis and comparison, we implement their backscatter modulations and designs in our platform and refer to our sub-symbol modulation based system as SubScatter. It is worth noting that HitchHike, SyncScatter, and SubScatter use different modulation methods. This work uses a sub-symbol level modulation method, whereas HitchHike and SyncScatter use a symbol level modulation method. To test the optimal performance of our system, we set the communication distance to 2 m and use an additional power supply. We present the experimental results in Fig. 5.12. The communication throughput of our system is 10.8 Mbps, which is much higher than the 0.25 and 0.99 Mbps of HitchHike and SyncScatter, respectively. HitchHike and SyncScatter have BER values of 0.13 and 0.21%, respectively, while our system has a BER value of 0.59%. Under the same experimental settings, the relatively higher BER of SubScatter is due to the higher synchronization requirements of sub-symbol level modulation and the faster data rate of the excitation signal. However, considering the significant improvement in throughput of sub-symbol level modulation, fine-grained and high-speed modulation is acceptable, even though it is more sensitive to noise and interference. Different FEC codes can be applied in tag data transmission for occasions with high decoding accuracy requirements to balance throughput and decoding accuracy. Furthermore, more precise synchronization methods will also reduce the impact of noise interference on the system. In conclusion, our proposed backscatter system can support high-definition video communication in the real world due to the high throughput and acceptable decoding accuracy.

5.6.2.3 FEC Effectiveness

We introduce the FEC codes in Sect. 5.4.3.5 to improve data transmission accuracy. By adding redundant bits to the real tag data, error correction can be achieved at the

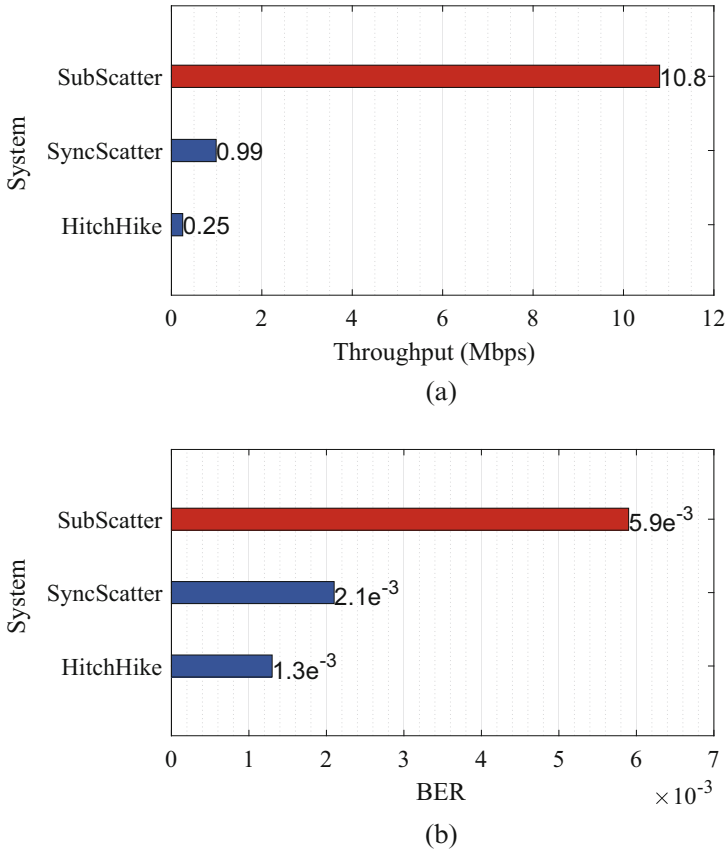


Fig. 5.12 The comparison of SubScatter with HitchHike and SyncScatter. (**a**) Throughput. (**b**) BER

receiver. In the experiment, we test several Hamming codes, including (7,4), (15,11), and (31,26), to study the effect of error correction codes on data transmission accuracy. When using the (31,26) Hamming code, the backscatter tag generates 31 bits of transmission tag data based on 26 bits of real tag data. Five redundant bits are used for verification and error correction of the 31-bit tag data decoded by the receiver. We test the PER performance in the tag data transmission to evaluate the effect of Hamming codes on decoding accuracy. The PER with the three Hamming codes is shown in Fig. 5.13.

Without error correction codes, PER exceeds 10%, and as the distance increases, data packets not affected by noise interference in the received packets are almost impossible to find. However, when Hamming codes with error correction capability are added to the tag data, we observe that PER significantly improves. The (7,4) code with the most robust error correction capability can achieve 10^{-3} level, while (15,11) and (31,26) can also achieve a PER of 1 and 2%, respectively. Among the

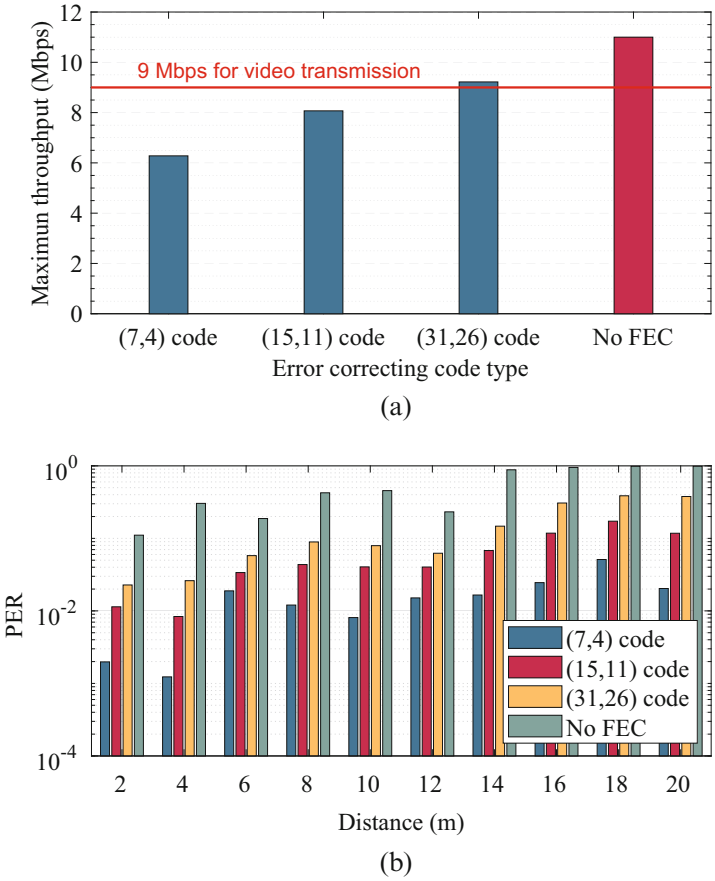


Fig. 5.13 The comparison of error correcting codes. (**a**) Throughput. (**b**) PER

three Hamming codes, (7,4) has the most robust error correction capability, so its decoding accuracy is higher than the other two Hamming codes. However, (7,4) Hamming code also has the lowest proportion of effective tag data among the three Hamming codes, which means that when the tag data length is the same, (7,4) Hamming code carries the least real tag data. Therefore, (7,4) Hamming code can be used when the data accuracy is high, such as in crucial information transmissions. FEC codes with fewer digits can be used for high-definition video transmission and other occasions with high data throughput requirements.

In addition, due to the requirement of verification after decoding data, adding an error correction code can have an impact on system efficiency. The additional time cost is related to the type and length of redundant codes. For example, when using parity bits, the receiver only needs to count the number of '1' in the decoded tag data, and the verification time is almost negligible. When using Hamming code, it is necessary to calculate the position of the error bit according to the verification

algorithm, and the computational complexity is related to the length. When the tag data is too long, the verification time may affect the efficiency of the system receiving tag data. In practical scenarios, the type and length of error correction bits need to be selected based on the trade-off of decoding accuracy and throughput.

5.7 Application Case

As urbanization continues to accelerate, communities are expanding in number and size. Traditional communities often cannot respond to unexpected events, leading to legal and economic disputes that cause great trouble for the community committee [42]. As management costs increase, the need for technological advancement becomes more pressing. This section proposes using an 802.11b Wi-Fi backscatter communication system for emergency services in communities to deal with unexpected situations.

For instance, older people in the community are often unaccompanied and cannot save themselves in accidents such as falls or slips, particularly during weekday working hours. Family members and neighbors may not discover their call for help in time, and community service workers may miss the best time to rescue them due to untimely access to information in traditional communities. Similarly, the intrusion of suspicious persons in the community may cause personal harm and economic loss as security personnel cannot detect and stop them. These unexpected events place a high demand on community management capabilities and response speed. Smart bracelets and smart emergency services using Wi-Fi backscatter technology can significantly improve this situation.

We propose the smart community design based on the 802.11b Wi-Fi backscatter system shown in Fig. 5.14. When an older person encounters an unexpected situation, a smart bracelet compatible with 802.11b Wi-Fi can send alert information, such as personal ID, location, and physiological indicators, to the community management cloud through backscatter communication based on symbol level modulation. Community managers can then use sub-symbol level modulation based HD video communication to understand the scene and contact community security. Depending on the level of urgency, local emergency centers and victims' families can be contacted. The community service staff with medical devices can then provide emergency treatment to older people at the accident scene, achieving the first response on time. Similarly, residents in the community who are robbed can send distress codes through smart devices. Based on-site videos and received distress messages, the intelligent cloud can assess the severity of the situation and arrange for security guards to drive away intruders and notify the police to rescue hostages.

Wi-Fi-based low-power backscatter communication technology ensures real-time connectivity between victims, community management cloud, community services, and emergency departments in smart communities. This scheme will improve community management efficiency while being compatible with existing

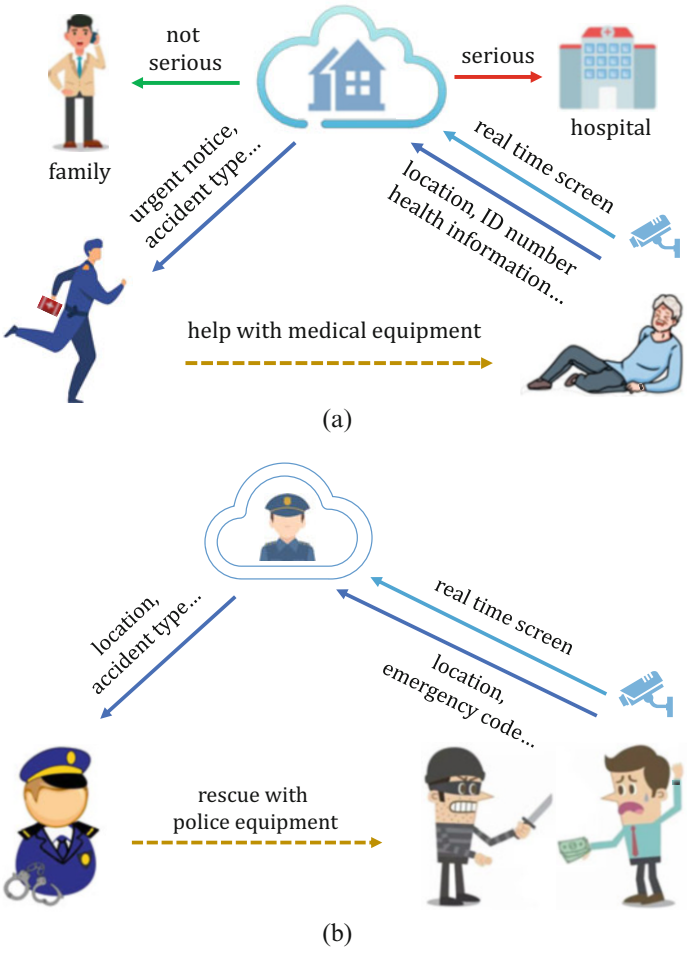


Fig. 5.14 The application cases of 802.11b Wi-Fi based backscatter system in smart community. (**a**) First aid. (**b**) Community security

infrastructure, reducing deployment, use, and maintenance costs. Furthermore, backscatter communication technology can be combined with other technologies, such as behavior recognition, to achieve more intelligent functions. Smart communities integrating these technologies, including cloud computing and artificial intelligence, can provide a safe and convenient modern living environment for community residents.

5.8 Summary

This chapter presents a backscatter system utilizing 802.11b Wi-Fi signals. This work first analyzes the shortcomings of existing 802.11b Wi-Fi-based backscatter systems, such as dependency on dedicated devices, low throughput, and high deployment costs. Next, the packet structure and modulation modes under different transmission rates in the 802.11b protocol are introduced. We then discuss the system's design and decoding methods based on symbol level modulation and sub-symbol level modulation from the perspective of modulation granularity. We build a prototype using off-the-shelf commercial devices to verify the feasibility and evaluate its key performance. The experimental results demonstrate the parallel transmission characteristics of CCK Wi-Fi and support high-definition video transmission with a throughput of up to 10.8 Mbps. We also discuss the error correction codes in tag data to ensure communication reliability. Finally, this work presents the potential of the backscatter system based on 802.11b Wi-Fi in emergency services in smart communities. In future work, we will focus on expanding fine-grained modulation schemes to other RF signals, such as OFDM-based 802.11n signals and FM-based Bluetooth.

References

1. Wang Q, Chen S, Zhao J, Gong W (2021) Rapidrider: efficient wifi backscatter with uncontrolled ambient signals. In: Proceedings of IEEE INFOCOM 2021 - IEEE conference on computer communications. IEEE, Piscataway, pp 1–10
2. Yang Y, Gong W (2022) Universal space-time stream backscatter with ambient wifi. In: Proceedings of 2022 IEEE international conference on pervasive computing and communications. IEEE, Piscataway, pp 101–110
3. Abedi A, Dehbashi F, Mazaheri MH, Abari O, Brecht T (2020) Witag: seamless wifi backscatter communication. In: Proceedings of the annual conference of the ACM special interest group on data communication on the applications, technologies, architectures, and protocols for computer communication, SIGCOMM'20. Association for Computing Machinery, New York, pp 240–252
4. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM. ACM, New York, pp 259–271
5. Iqbal A, Olariu S (2021) A survey of enabling technologies for smart communities. Smart Cities 4(1):54–77
6. Azgomi HF, Jamshidi M (2018) A brief survey on smart community and smart transportation. In: 2018 IEEE 30th international conference on tools with artificial intelligence (ICTAI), pp 932–939
7. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of the 13th international conference on emerging networking experiments and technologies. ACM, New York, pp 389–401
8. Dunna M, Meng M, Wang PH, Zhang C, Mercier P, Bharadia D (2021) Syncscatter: enabling wifi like synchronization and range for wifi backscatter communication. In: Proceedings of 18th USENIX symposium on networked systems design and implementation. USENIX, pp 923–937

9. IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan networks - specific requirements - part 11: wireless lan medium access control (MAC) and physical layer (phy) specifications: higher speed physical layer (phy) extension in the 2.4 Ghz band (2000). IEEE Std 802.11b-1999, pp 1–96
10. Yuan L, Gong W (2022) Subscatter: sub-symbol wifi backscatter for high throughput. In: 2022 IEEE 30th international conference on network protocols (ICNP). IEEE, Piscataway, pp 1–11
11. Boyer C, Roy S (2014) Backscatter communication and RFID: coding, energy, and MIMO analysis (invited paper). IEEE Trans Commun 62(3):770–785
12. Sample AP, Yeager DJ, Powledge PS, Mamishev AV, Smith JR (2008) Design of an RFID-based battery-free programmable sensing platform. IEEE Trans Instrum Measur 57(11):2608–2615
13. Sample AP, Yeager DJ, Powledge PS, Smith JR (2007) Design of a passively-powered, programmable sensing platform for UHF RFID systems. In: 2007 IEEE international conference on RFID
14. Liu V, Parks A, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. SIGCOMM Comput Commun Rev 43(4):39–50
15. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In: Proceedings of the 2016 ACM SIGCOMM conference. ACM, New York, pp 356–369
16. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In: Proceedings of the 13th USENIX conference on networked systems design and implementation, NSDI'16. USENIX Association, New York, pp 151–164
17. Zhang P, Bharadia D, Joshi K, Katti S (2016) Enabling backscatter communication among commodity wifi radios. In: Proceedings of the 2016 ACM SIGCOMM conference, SIGCOMM'16. Association for Computing Machinery, New York, pp 611–612
18. ZhaoJ, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of the 16th annual international conference on mobile systems, applications, and services. ACM, New York, pp 191–203
19. Zhang M, Zhao J, Chen S, Gong W (2020) Reliable backscatter with commodity BLE. In: Proceedings of IEEE INFOCOM 2020-IEEE conference on computer communications. IEEE, Piscataway, pp 1291–1299
20. Zhang M, Chen S, Zhao J, Gong W (2021) Commodity-level BLE backscatter. In: Proceedings of the 19th annual international conference on mobile systems, applications, and services. IEEE, Piscataway, pp 402–414
21. Chen S, Zhang M, Zhao J, Gong W, Liu J (2021) Reliable and practical bluetooth backscatter with commodity devices. IEEE/ACM Trans Netw 29(4):1717–1729
22. Huang Z, Gong W (2022) Eascatter: excitor-aware bluetooth backscatter. In: 2022 IEEE/ACM 30th international symposium on quality of service (IWQoS), pp 1–10
23. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of ACM SIGCOMM
24. Li Y, Chi Z, Liu X, Zhu T (2018) Passive-zigbee: enabling zigbee communication in IoT networks with 1000x+ less power consumption. In: Proceedings of the 16th ACM conference on embedded networked sensor systems. ACM, New York, pp 159–171
25. Xu Z, Gong W (2022) Enabling zigbee backscatter communication in a crowded spectrum. In: 2022 IEEE 30th international conference on network protocols (ICNP), pp 1–11
26. Xu Z, Ding Y, Gong W (2022) A fine-grained modulation technology for zigbee backscatter communication. In: 2022 microwave mediterranean symposium (MMS), pp 1–4
27. Wang A, Iyer V, Talla V, Smith JR, Gollakota S (2017) FM backscatter: enabling connected cities and smart fabrics. In: Proceedings of the 14th USENIX conference on networked systems design and implementation. USENIX, New York, pp 243–258
28. Gong W, Liu J, Yang Z (2017) Efficient unknown tag detection in large-scale RFID systems with unreliable channels. IEEE/ACM Trans Netw 25(4):2528–2539

29. Zhao J, Gong W, Liu J (2020) Towards scalable backscatter sensor mesh with decodable relay and distributed excitation. In: Proceedings of the 18th international conference on mobile systems, applications, and services. ACM, New York, pp 67–79
30. Gong W, Yuan L, Wang Q, Zhao J (2020) Multiprotocol backscatter for personal IoT sensors. In: Proceedings of the 16th international conference on emerging networking experiments and technologies. ACM, New York, pp 261–273
31. Liu H, Gong W, Chen L, He W, Liu K, Liu Y (2014) Generic composite counting in RFID systems. In: 2014 IEEE 34th international conference on distributed computing systems, pp 597–606
32. Daskalakis SN, Kimionis J, Collado A, Tentzeris MM, Georgiadis A (2017) Ambient FM backscattering for smart agricultural monitoring. In: 2017 IEEE MTT-S international microwave symposium (IMS), pp 1339–1341
33. Daskalakis SN, Assimonis SD, Goussetis G, Tentzeris MM, Georgiadis A (2019) The future of backscatter in precision agriculture. In: 2019 IEEE international symposium on antennas and propagation and USNC-URSI radio science meeting, pp 647–648
34. Talla V, Hessar M, Kellogg B, Najafi A, Smith JR, Gollakota S (2017) Lora backscatter: enabling the vision of ubiquitous connectivity. Proc ACM Interact Mob Wearable Ubiquitous Technol 1(3):1–24
35. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) Plora: a passive long-range data network from ambient lora transmissions. In: Proceedings of the 2018 conference of the ACM special interest group on data communication. ACM, New York, pp 147–160
36. Zhao J, Gong W, Liu J (2018) X-tandem: towards multi-hop backscatter communication with commodity wifi. In: Proceedings of the 24th annual international conference on mobile computing and networking. ACM, New York, pp 497–511
37. Li X, Lu R, Liang X, Shen X, Chen J, Lin X (2011) Smart community: an internet of things application. IEEE Commun Mag 49(11):68–75
38. Lwowski J, Kolar P, Benavidez P, Rad P, Prevost JJ, Jamshidi M (2017) Pedestrian detection system for smart communities using deep convolutional neural networks. In: 2017 12th system of systems engineering conference (SoSE), pp 1–6
39. Jameel F, Duan R, Chang Z, Liljemark A, Ristaniemi T, Jantti R (2019) Applications of backscatter communications for healthcare networks. IEEE Netw 33(6):50–57
40. Jameel F, Zeb S, Khan WU, Hassan SA, Chang Z, Liu J (2020) NOMA-enabled backscatter communications: toward battery-free IoT networks. IEEE Internet Things Mag 3(4):95–101
41. Stigge M, Plötz H, Müller W, Redlich JP (2006) Reversing CRC–theory and practice, vol 17. Humboldt University Berlin, Berlin
42. Azgomi HF, Jamshidi M (2018) A brief survey on smart community and smart transportation. In: 2018 IEEE 30th international conference on tools with artificial intelligence (ICTAI), pp 932–939

Chapter 6
Content-Agnostic Backscatter with Ambient OFDM Signals

Abstract This chapter provides a content-agnostic backscatter system that demodulates both ambient data and tag data only from backscattered Wi-Fi. The system, CAB, overcomes the limitations of either have low throughput or use the additional receivers to demodulate tag data. Unlike previous ambient backscatter systems using ambient data to carry tag data, CAB utilizes zero-subcarriers to transmit tag data. The idea behind our approach is simple and elegant, as zero-subcarrier is invariant and independent for ambient OFDM Wi-Fi signal. In traditional ambient backscatter systems, decoding data is difficult due to unknowable ambient backscatter content, and redundant modulation limits the system's performance. However, CAB overcomes these issues. To verify the effectiveness of CAB, we prototype it using FPGAs and SDRs and conducted extensive experiments. The performance of CAB is high, and the aggregate throughput is up to 340.9 Mbps, achieving 97% of Shannon capacity.

6.1 Introduction

In this section, we provide an overview of the main features of ambient backscatter communication. We also examine the challenges faced by current ambient backscatter systems. Finally, we introduce the concept of zero-subcarriers and discuss the key technical hurdles that must be overcome to implement CAB.

In recent years, ambient backscatter has garnered significant attention due to its potential to provide near-zero power communication for a large number of small devices [1–10]. This communication method differs from traditional RFID communication in several ways. Firstly, it utilizes uncontrolled ambient signals as carriers. Secondly, it offers high throughput backscatter communications with data rates that are considerably higher than those of RFID systems [11, 12]. Lastly, ambient backscatter doesn't require a specialized full-duplex radio for decoding, as a standard radio supporting a common wireless protocol suffices [13–15]. This ease of integration into existing wireless communication systems reduces the need for dedicated hardware and the cost of deployment, making it a highly attractive option.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_6

While the independence of the excitation source and receiver allows ambient backscatter to be widely used, uncontrolled ambient signals pose challenges for demodulating tag data [2, 16]. In traditional wireless communication systems, demodulation relies on finding the difference between the reference signal and the received signal [17]. However, in ambient backscatter, finding a reference for demodulation becomes the key challenge.

Existing ambient backscatter systems use a content-aware approach, employing an additional receiver to capture ambient data used as a reference to demodulate the tag data. However, this content-aware approach has some drawbacks. Firstly, the demodulation of tag data is entirely dependent on the quality of the ambient data. Secondly, the demodulation process uses two separate frequency bands, resulting in the channel bandwidth not being fully utilized. Finally, this approach introduces additional hardware costs and synchronization costs between the two receivers.

Faced with the problem of content-aware systems, we wondered how to demodulate tag data only from ambient backscattered signals? If it is possible, tag can reuse the abundant but unknown ambient signals as excitations, and a single srandard radio is sufficient to demodulate backscattered signal. This means we have taken an important step towards pervasive ambient backscattering. However, if the ambient signal is not available, there will be no reference for demodulating tag data, so designing such a system is extremely challenging.

We have a profound discovery: zero-subcarriers are natural-born invariants. Specifically, no matter what data is modulated on OFDM Wi-Fi signals, zero-subcarriers remain the same: single tones. Based on the perfect reference signals, we propose CAB, that can demodulate tag data and ambient data from backscattered signal, respectively. Compared with existing systems, CAB novelly uses the zero subcarrier to backscatter tag data, as shown in Fig. 6.1. CAB not only overcomes the dilemma that demodulation of tag data depends on ambient data, but also takes

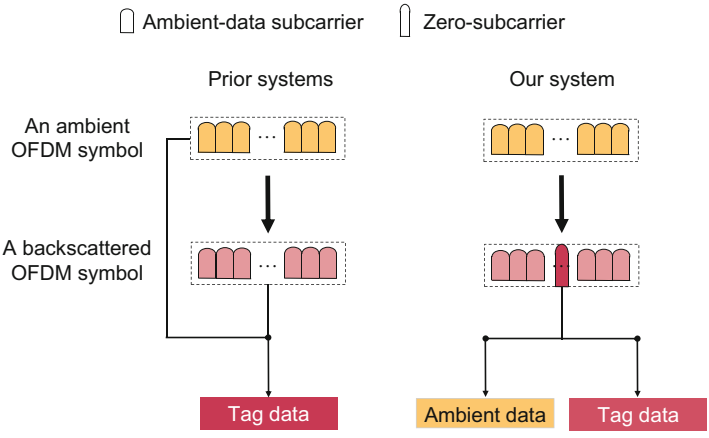


Fig. 6.1 Comparison between our system and prior systems

a step towards improving the practicability of ambient backscatter due to expanded excitation source and reduced data demodulation cost. In order to implement such a system, we face several key challenges.

The first challenge is how to accurately estimate the phases of zero-subcarriers and demodulate tag data from them. In theory, the phases of backscattered signals from zero-subcarriers should be identical to the phase rotations caused by tag modulation. However, obtaining these values directly on typical Wi-Fi receivers is not possible. We propose an approach based on Weighted-Least-Square (WLS) for phase estimation.

The second challenge involves the demodulation of ambient data without prior knowledge of tag data. Our approach diverges from traditional phase tracking methods employed in standard Wi-Fi by introducing a pre-filter. This pre-filter is designed to calibrate the CPE and phase rotations of tag data on a symbol-by-symbol basis. Thanks to this calibration, we achieve notably low BERs when decoding ambient data. A detailed explanation of our approach is provided in Sect. 6.4.

The third challenge pertains to achieving sub-symbol level synchronization of the tag. In order to accurately demodulate, it is necessary to have precise pilot and data subcarriers which in turn require sub-symbol level synchronization accuracy for tag modulation. This task is challenging because Wi-Fi demodulation on tags is not feasible, rendering conventional training fields such as the legacy short training field (L-STF) useless. We propose a joint synchronization method that leverages the high-precision independent demodulation technique discussed in Sect. 6.4. We assign most of the computational burden to the receiver, while the tag only needs to perform a simple interval search. A detailed workflow is elucidated in Sect. 6.4.

6.2 Related Work

We will explore the development of ambient backscatter technology, which can be devided into two types based on the type of excitation used: content-agnostic backscatter and content-aware backscatter.

Ambient backscatter [2] proposes to realize battery-free backscatter communication using TV signals in a pioneering way. Later, Wi-Fi backscatter [13] extends this idea to Wi-Fi signals, achieving the first universal Wi-Fi backscatter. FS-backscatter [5] discovers that frequency shifting is key to improving demodulation accuracy, while systems that employ packet-level modulation are only able to achieve low data throughput of up to thousands of bps.

In contrast, HitchHike [16] pioneers the use of symbol-level modulation and codeword translation to modulate and demodulate tags using uncontrolled 802.11b ambient signals as carriers, achieving a throughput of about 300 kbps. This approach inspires later developments such as MoXcatter [18], X-Tandem [19], PLoRa [20], Lscatter [11], and Tscatter [12]. Unlike these systems, which rely on ambient data to demodulate, [21] demodulates tag data without knowing the ambient

data. Meanwhile, it adopts subsymbol-level modulation to achieve an aggregate throughput of up to 340.9 Mbps.

In summary, ambient backscatter technology has made significant strides in recent years. While earlier systems employ packet-level modulation, more recent developments have utilized symbol-level modulation and codeword translation to achieve higher data throughput. However, the reliance on ambient data for demodulation remains a significant challenge for these systems.

6.3 Background

We first briefly introduce the basic concepts of ambient backscatter system, and then, we focus on the basic idea of CAB: zero-subcarrier.

6.3.1 Ambient Backscatter System

In a typical ambient backscatter system, there are three main components: an excitor that provides carriers for tag modulation; a tag that synchronizes with the carrier and backscatters it to transmit data to a receiver; and a receiver that demodulates the backscattered signals. In traditional RFID communications, the reader acts as both the excitor and receiver. Despite researchers' attempts to decouple the excitor and receiver in ambient backscatter systems in recent years, they remain somewhat connected, for instance, requiring two receivers to receive the excitation signal and backscatter signal, respectively [12, 16]. Our objective is to completely disengage them.

6.3.2 Basic Idea

Departing from previous systems that have attempted to deal with the changing excitations, as evidenced by studies such as [12, 16, 18, 19], we have adopted a new approach to this problem. Our hypothesis is that if we can identify invariants within variant signals, those uncontrolled signals can be considered as a type of "continuous wave". We have discovered that all OFDM Wi-Fi signals around us contain virtual invariants.

For instance, consider the structure of a Wi-Fi 4 symbol, shown in Fig. 6.2a. For 20 MHz bandwidth operation, a symbol in this system comprises 64 subcarriers. Among them, 52 subcarriers are allocated for data transmission, 4 serve as pilot subcarriers for precise channel estimation, one is reserved for DC, and the remaining seven act as guard bands. We have observed that the four pilot subcarriers, being

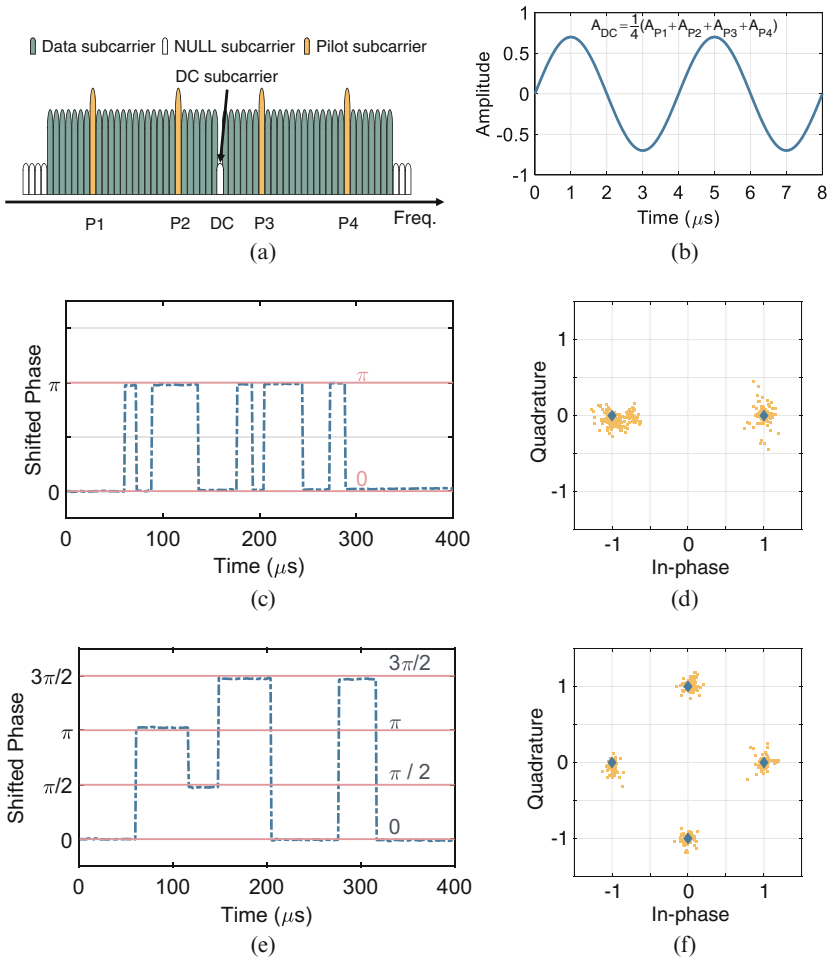


Fig. 6.2 Our key insight of the system design. (**a**) Wi-Fi symbol structure. (**b**) Virtual zero-subcarrier's waveform. (**c**) Backscattered BPSK. (**d**) Constellation diagram. (**e**) Backscattered QPSK. (**f**) Constellation diagram

known and fixed, can be used to create a virtual subcarrier at their center, which is null, i.e., no signals are transmitted on it. We call this subcarrier the zero-subcarrier, and its phase and magnitude can be estimated from the pilot subcarriers. In Fig. 6.2b, the visualization results of zero-subcarriers are presented. These zero-subcarriers are obtained by averaging the four pilots from an uncontrolled excitations. The visualization reveals a single tone at 250 kHz, which is an optimal choice.

To explore the behavior of the tag, we enable it to modulate the uncontrolled Wi-Fi packet using Binary PSK (BPSK). At the receiver side, we closely observe the phases of the zero-subcarriers. Figure 6.2c illustrates that the backscattered zero-

subcarriers exhibit two distinct levels of phase. Furthermore, the corresponding constellation diagram in Fig. 6.2d clearly shows two separate clusters, confirming the presence of BPSK signals. Similar findings were observed in Figs. 6.2e, f when the tag modulates using Quadrature PSK (QPSK). The examples provided highlight the capability of virtual zero-subcarriers to operate as continuous waves. This implies that within every OFDM Wi-Fi ambient signal, there exists a concealed single tone.

6.4 CAB Design

In this section, we first give an overview of our CAB framework. Then, based on the phase expression of the received signal, we introduce how to estimate the zero-subcarrier and separate the CPE, so as to demodulate the tag data and further demodulate ambient data. Finally, we explain the implementation of sub-symbol synchronization.

6.4.1 Overview

CAB aims to transmit tag data by leveraging ambient OFDM Wi-Fi excitation signals. When receiving the excitation signal, the tag embed sensing data by PSK modulation. In order to avoid interference on the original channel, the backscatter signals are shifted to another Wi-Fi channel by the tag [5]. After receiving the backscattered signal, the receiver's goal is to demodulate the tag data without knowing the ambient data, and at the same time demodulate the ambient data from the backscattered signal. We first give a formal formulation of the problem. The received phase for subcarrier j from received symbol i is expressed as follows:

$$\phi_{i,j}^{r} = \phi_{i,j}^{am} + \phi_{i,j}^{ch} + \phi_{i,j}^{cfo} + \phi_{i,j}^{sto} + \phi_{i,j}^{sfo} + \phi_{i,j}^{tag}. \tag{6.1}$$

where ϕ^{am}, ϕ^{ch}, ϕ^{cfo}, ϕ^{sto}, ϕ^{sfo}, and ϕ^{tag} represent the phase rotations of corresponding operations. Next, the methodology for extracting ϕ^{tag} and ϕ^{am} from ϕ^{r} is presented.

6.4.2 Tag-Data Demodulation

In this section, we focus on the phases of zero-subcarriers, $\phi_{i,0}^{r}$. This approach has several benefits. Firstly, the absence of ambient data transmission on this subcarrier [22–26] and its virtual single-tone nature make $\phi_{i,0}^{am} = 0$ [17]. Secondly,

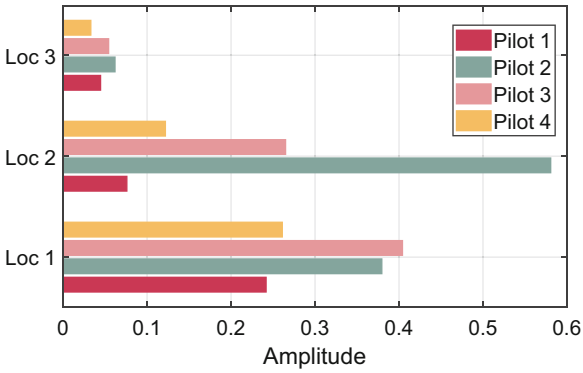


Fig. 6.3 Diverse pilot qualities at different locations

except for the zero-subcarrier, STO and SFO affect all the subcarriers, making $\phi_{i,0}^{sto} = 0, \phi_{i,0}^{sfo} = 0$ [27, 28]. Since the preamble of the excitation packet remains unchanged, such as the short- and long-training fields (S-LTF and L-LTF), are preserved. Equation 6.2 shows the received zero-subcarrier phase before demodulation:

$$\phi_{i,0}^{r} = \phi_{i,0}^{cpe} + \phi_{i,0}^{tag}, \tag{6.2}$$

where $\phi_{i,0}^{cpe}$ is the phase rotation [29, 30], known as the "common phase error" (CPE).

To achieve accurate phase estimation, we show the two key steps:

Phase Estimation for Zero-Subcarriers Accurately estimating the phase for zero-subcarriers is crucial in the demodulation of tag data. While simple averaging or spline interpolation across all pilots may seem like straightforward methods for obtaining zero-subcarrier phases [28], they are inadequate for demodulation purposes. As demonstrated in Fig. 6.3, SNRs of pilots exhibit significant differences at different locations. The uneven quality of pilot phases causes scattered constellation points, as shown in Fig. 6.5(a). This motivates our approach to account for this variability. Specifically, we perform this procedure for the k-th symbol:

$$\arg\min_{\beta_0,\beta_1} \Sigma_{i=1}^{n_p} A_i(\Phi_i - \beta_0 - \beta_1 x_i)^2. \tag{6.3}$$

We let n_p denote the pilot count, and A_i, Φ_i and x_i denote the magnitude, phase and index of the i-th pilot, respectively. Through this process, we obtain the estimated phase for the zero-subcarrier, denoted as $\widehat{\phi_{k,0}^{r}}$, as well as the slope of the approximated linear equation, denoted as β_1. This slope provides insights into the impact of STO on the pilots. The WLS method results in a tightly gathered constellation points around a circle, as seen in Fig. 6.5b. However, errors from CPE for $\widehat{\phi_{k,0}^{r}}$ still need to be addressed in our subsequent step.

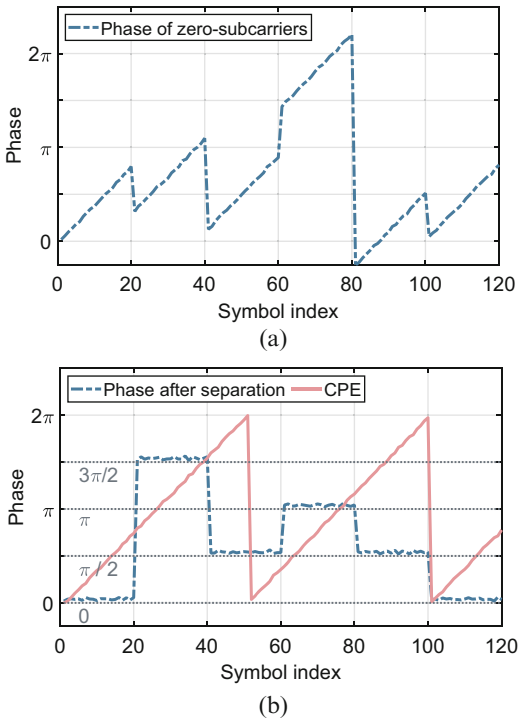


Fig. 6.4 Phase performance before and after the CPE separation operation. (**a**) Before separation. (**b**) After separation

CPE Separation Firstly, CPE is deeply intertwined with tag-data phase rotations, as shown in Eq. 6.1, which has been barely discussed in prior ambient backscatter systems [2, 5, 12]. Furthermore, traditional CPE calibration schemes in Wi-Fi receivers [27, 29, 30] are unable to handle this issue as they are designed to operate effectively only in scenarios where there is no involvement of tag-data induced phase.

We design an iterative CPE separation scheme to address the above challenges. For each symbol, we perform the following steps:

1. The CPE estimate is assigned from the symbol $(i-1)$ to the symbol (i), $\widehat{\phi_{i,0}^{cpe}} \leftarrow \widehat{\phi_{i-1,0}^{cpe}}$, with the exception of the first symbol, which is assigned a CPE of zero, $\widehat{\phi_{1,0}^{cpe}} = 0$.
2. Use Eq. 6.2, $\widehat{\phi_{i,0}^{tag}} \leftarrow \widehat{\phi_{i,0}^{r}} - \widehat{\phi_{i,0}^{cpe}}$ to estimate the tag-data phase, and then update it to the phase of its nearest constellation center.
3. Use the new tag-data phase estimate to update the CPE.

This iterative process is repeated for each symbol, successfully removing the accumulating CPE, as demonstrated in Fig. 6.4. Through our approach, we achieve successful separation of the CPE, resulting in the elimination of accumulating

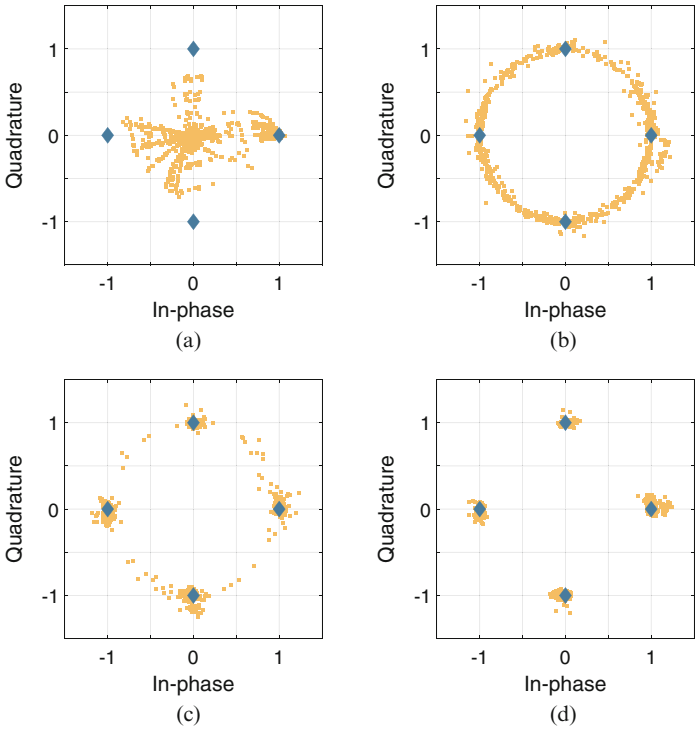


Fig. 6.5 Demodulation process of tag data. (**a**) Simple averaging. (**b**) WLS. (**c**) CPE separation. (**d**) Symbol assembly

errors within the respective segments post-separation. We observe distinct clusters resembling tag-data modulation points, as visually depicted in Fig. 6.5c. This significant outcome validates the effectiveness of our approach. The demodulation task for tag-data is nearly complete, thanks to our proposed iterative CPE separation scheme.

Symbol Assembly In Fig. 6.5c, it can be observed that there are some stragglers caused by SFO. SFO arises when there is a discrepancy between the sampling frequency of the transmitter and that of the receiver. In the case of a 20 MHz transmission, the Wi-Fi receiver is expected to sample 80 points for a 4 μs OFDM symbol. We leverage the use of β_1 as a reliable indicator of STO to coordinate symbol assembly.

The tag-data demodulation process is shown below: The receiver initially receives the backscattered signal and performs several calibration steps. Once the initial calibrations are completed, the receiver proceeds to estimate the phases of zero-subcarriers for each symbol. It employs an iterative approach to separate the tag-data phases from CPEs. Simultaneously, the receiver accurately assembles the

OFDM symbols by approximating the STO caused by SFO. Finally, the receiver recovers the tag data by demapping the received signals to the closest constellation centers. Figure 6.5d illustrates the demodulated data, which displays a clear QPSK constellation without any distortion or rotation, indicating an exceptionally low BER. This comprehensive demodulation process ensures the successful recovery of tag data from the backscattered signals, achieving high accuracy and minimal bit errors.

6.4.3 Ambient-Data Demodulation

When demodulating ambient data, we do not want to rely on demodulated tag data. If the tag data is unknown, we find that the challenge of demodulation ambient data is that each symbol encounters diverse channel conditions due to the modulation of tag data. This phenomenon is particularly evident in two areas.

Pilot Averaging Over Symbols In standard Wi-Fi, pilot averaging over a sliding window is commonly employed to address the effects of varying STO caused by SFO [29]. While this approach is effective for standard Wi-Fi, it does not work for backscattered signals. Figure 6.6 illustrates the issue where Symbol $i-1$ and Symbol $i+1$ modulated with a tag phase of π exhibit different channel conditions compared to other symbols. Consequently, the averaged pilots of these symbols deviate from the expected mean.

Inter-Symbol Phase Unwrapping It is a standard operation in Wi-Fi that involves calculating the rate at which phase errors induced by SFO rotate across different subcarriers [29].

The difficulties mentioned earlier seem to make it almost impossible to demodulate ambient data without prior knowledge of the tag data. However, a different perspective unveils a potential solution: can we eliminate tag-data phase rotations without having access to the tag data itself? The answer is affirmative. As discussed in Sect. 6.4.2, the phase induced by tag data is closely intertwined with CPE in the zero-subcarrier phase. Therefore, by subtracting the zero-subcarrier phase from all

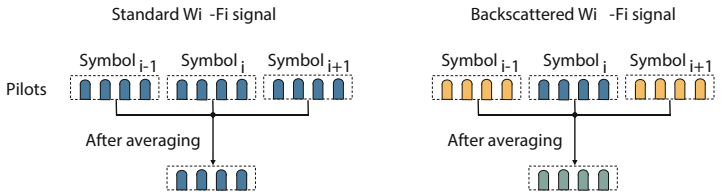


Fig. 6.6 Pilot averaging for standard Wi-Fi signal and backscatter Wi-Fi signal

subcarriers within a symbol, we can implicitly eliminate the tag-data phase rotation, irrespective of the modulation scheme employed for the tag data. Furthermore, given that the incorrect phase unwrapping and pilot averaging in backscattered Wi-Fi signals mainly originate from cross-symbol operations, it is essential to perform the subtraction process on a symbol-by-symbol basis. This approach ensures that the necessary corrections are applied specifically within each symbol, mitigating any potential errors caused by inter-symbol interference.

Drawing upon this understanding, we present a novel phase tracking scheme that encompasses a pre-filter capable of calibrating both the CPE and tag-data phase rotations. By incorporating this pre-filter, we enable standard Wi-Fi phase tracking to effectively recover all the ambient data. Consequently, the actual CPE values will not be deducted twice, ensuring accurate calibration of the CPE and avoiding any potential redundancies.

6.4.4 Subsymbol-Level Synchronization

Achieving accurate subsymbol-level synchronization is crucial for CAB to enable the successful recovery of zero-subcarriers and data-subcarriers by the receiver. Traditional Wi-Fi receivers encounter no issues with synchronizing to Wi-Fi signals due to the presence of dedicated training fields [22, 24–26]. However, current tags are unable to decode these fields, rendering them unusable. Consequently, previous systems approach this challenge in various ways. Existing approaches, such as Hitchhike [16], FreeRider [15], and their variations [18, 19], employ energy detection as a coarse synchronization method. However, these methods do not operate at the level of OFDM subcarriers.

Figure 6.7 shows the BER performance with different synchronization offsets, which can be used as one of the indicators of synchronization effect, as we discussed in Sect. 6.4.3. We propose our solution as follows.

Tag Side To achieve synchronization with the ambient Wi-Fi packet, the tag employs an energy detector for initial coarse synchronization. For fine-grained

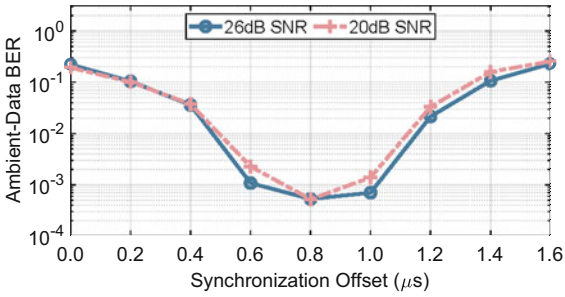


Fig. 6.7 BER comparison for different synchronization offsets

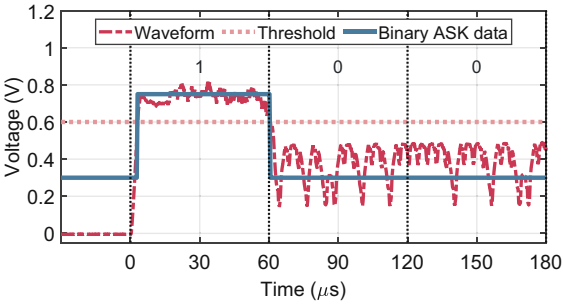


Fig. 6.8 Communication between tag and receiver

synchronization, our approach involves initiating an interval search. The search begins τ seconds after the coarse start, where τ denotes the time length before the PSDU and the MAC header. The step size of the search is set to $\frac{1}{2}$ of the Guard Interval (GI) length. The search window length is 1 symbol, which is sufficient given the error of our coarse start, which is approximately 2 μs, consistent with prior systems [16, 18]. If the received message is 'S-ACK', the tag considers the current search point as accurate. However, if the received message differs, the tag progresses to the next search point, continuing the search process. To enhance the efficiency of our search process, a multi-resolution approach can be employed. This involves utilizing different step sizes at various layers, specifically $\frac{1}{2}$ of the GI and $\frac{1}{20}$ of the GI, respectively. This multi-resolution strategy facilitates a more refined and comprehensive search, allowing for increased accuracy and effectiveness in identifying the optimal synchronization point.

Receiver Side When a backscattered packet is received, the receiver employs the method described in Sect. 6.4.3 to demodulate ambient data. To decide whether to send an 'S-ACK' (indicating successful synchronization), the receiver needs to set a threshold according to the communication situation. However, in our design, the receiver operates independently from the exciters, making it challenging to directly obtain the groundtruth bits for the ambient data and compute the Bit Error Rate (BER). To overcome this limitation, we leverage the CRC. Although the CRC field was originally intended to detect unintentional alterations to raw data, it can also serve as a reliable indicator of the wireless demodulation quality [17]. Therefore, if the backscattered packet successfully passes the CRC verification, signaling a successful demodulation, the receiver transmits an 'S-ACK' to the tag. Conversely, if the CRC verification fails, indicating a CRC error, the receiver sends an 'F-ACK' to the tag. This approach allows us to indirectly assess the demodulation performance and provide feedback to the tag without directly computing the BER. The CRC field can also serve as By utilizing the CRC field in this manner, the receiver can effectively determine the synchronization status without direct access to the groundtruth bits of the ambient data.

Tag-RX Communication We leverage the concept introduced in Interscatter [31] that enables the transformation of OFDM symbols into ASK-modulated signals. Remarkably, the tag can demodulate these Wi-Fi-emulated ASK signals by an envelope detector and filter. Figure 6.8 illustrates the process by which a low-power tag performs this task, wherein a comparator separates the waveform received from the filter into its low-energy and high-energy components, thereby generating binary signals.

6.5 Performance Evaluation

6.5.1 Implementation

Receiver Prototype We use ZedBoard ZYNQ-7000 [32] and AD-FMCOMMS3 [33] to prototype our Wi-Fi receiver. We implement different Wi-Fi standards.

Tag Prototype for Verification We develop a functional verification prototype, illustrated in Fig. 6.9a.

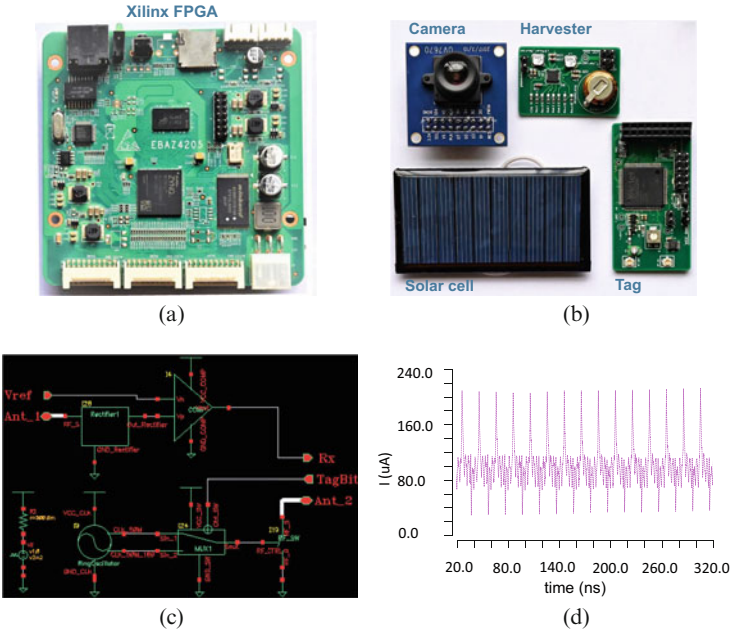


Fig. 6.9 The FPGA prototype and IC simulation of our system. (**a**) Verification prototype. (**b**) Battery-free prototype. (**c**) IC simulated circuit. (**d**) Currents of IC simulation

Table 6.1 Power consumptions of three prototypes

	Power consumption breakdown				
	Digital core	Oscillator	RF-switch	Detector	Total
Verification	209.00 mW	18.15 mW	1.83 mW	78.00 mW	307.03 mW
Battery-free	5.85 mW	0.59 mW	1.83 mW	0.18 mW	8.45 mW
IC	39.00 μW	196.00 μW	2.41 μW	33.79 μW	271.20 μW

Tag Prototype for Applications We have also developed a prototype that utilizes low-power devices for a battery-free backscatter camera, which is demonstrated in Fig. 6.9b.

Tag Prototype with IC The power consumption analysis in Table 6.1 reveals that the battery-free prototype exhibits a significantly lower power consumption of 8.45 mW compared to the verification prototype's 291 mW. To further realize CAB's ultra-low power capabilities, we perform simulations using Cadence IC6.17 Virtuoso software and TSMC 0.18 μm CMOS process design kits. IC prototype consists primarily of an RF front end, oscillator, and digital core, illustrated in Fig. 6.9(c).

Figure 6.9d shows that the average current is approximately 116.10 μA. Notably, the oscillator contributes significantly to the power dissipation, indicating that there is still room for further power optimization using advanced IC techniques [34, 35].

6.5.2 Evaluation

Initially, we assess the end-to-end performance of CAB with various Wi-Fi signals using the functional verification prototype, followed by analyzing the influence of each algorithm. Finally, we showcase the practical implementation of the battery-free prototype.

6.5.2.1 End-to-End Performance

Since CAB is intended to work with diverse OFDM Wi-Fi signals, we aim to evaluate its general performance across various Wi-Fi traffic types, such as multi-band, multi-stream, and multi-user Wi-Fi.

Wi-Fi 3 We first examine the effectiveness of CAB with a typical single-stream OFDM Wi-Fi setup. Excitations are transmitted at −10 dBm in a 20 MHz band, where the GI is 0.8 μs. Figure 6.10 shows that the throughputs for ambient data for modulation are 100% ($\frac{6}{6}$), 100% ($\frac{18}{18}$), 97.1% ($\frac{34.96}{36}$), and 99.8% ($\frac{53.94}{54}$) of their

	MCS index				Excitation modulation	Wi-Fi 3			Wi-Fi 4		Wi-Fi 5		Wi-Fi 6	
	Non-HT[1]	HT[2]	VHT[3]	HE[4]		T/BPSK[5]	T/QPSK	T/16PSK	20MHz	40MHz	Single stream	Double streams	1 user with 484 tones	2 users, 242 tones each
Ambient-data	13	0	0	0	BPSK	6.00[6]	6.00	6.00	7.20	14.96	14.99	30.00	34.40	34.35
	7	2	2	2	QPSK	18.00	18.00	17.99	21.70	44.42	44.91	89.58	102.20	102.11
	11	4	4	4	16QAM	34.93	34.96	34.94	43.30	89.00	89.70	179.83	204.04	205.96
	3	7	7	7	64QAM	53.94	53.90	53.75	72.06	145.78	148.63	294.70	340.61	327.66
Tag-data	13	0	0	0	BPSK	0.25	0.50	0.98	1.08	1.09	1.08	1.07	0.29	0.21
	7	2	2	2	QPSK	0.25	0.50	0.98	1.08	1.09	1.07	1.06	0.29	0.22
	11	4	4	4	16QAM	0.25	0.50	0.98	1.10	1.09	1.08	1.10	0.29	0.22
	3	7	7	7	64QAM	0.25	0.50	0.98	1.10	1.10	1.09	1.09	0.29	0.22

Fig. 6.10 Throughput comparison of CAB for different excitations

MCS capacities. The maximal tag-data throughputs are 0.25, 0.5, and 0.99 Mbps for BPSK, QPSK, and 16PSK tag modulations, respectively.

Wi-Fi 4 We proceed to investigate the performance of CAB with multi-band Wi-Fi 4 signals, using 16PSK tag-data modulation and a shortened GI of 0.4 μs. In a 40 MHz band, we observe from Fig. 6.10 that the ambient data throughput nearly doubles compared to the 20 MHz band, confirming CAB's compatibility with Wi-Fi's high-throughput designs. Moreover, the introduction of the short GI boosts to 1.1 Mbps.

Wi-Fi 5 Building on the high-throughput parameters used in Wi-Fi 4 experiments (short GI and 40 MHz band), we evaluate CAB's performance with multi-stream Wi-Fi 5 signals. We find that the results of single-stream traffic are similar to those with Wi-Fi 4. However, the maximal ambient-data throughput improves to 294.70 Mbps.

Wi-Fi 6 To further explore the capabilities of CAB in ambient Wi-Fi backscatter, we investigate its potential with Wi-Fi 6 signals. The results demonstrate that CAB performs smoothly with Wi-Fi 6 excitations, as depicted in Fig. 6.10. Specifically, the maximal throughput for ambient data transmission reaches 340.61 Mbps, thanks to the reduced equivalent GI of Wi-Fi 6, which is only 0.2 μs ($\frac{0.8}{4}$). Despite the longer symbol length of 13.6 μs in Wi-Fi 6, which leads to a decrease in tag-data throughput, we are still able to achieve a remarkable aggregate throughput of 340.9 Mbps. This is accomplished using 64QAM Wi-Fi 6 excitation and tag modulation with 16PSK, which represents 97% ($\frac{340.9}{351.38}$) of the Shannon capacity.

The evaluation presented above provides a thorough examination of CAB's performance with various types of OFDM Wi-Fi excitations, showcasing its universality, high throughput, and independence from modulation schemes.

Competitions We compare CAB with three existing systems, FS-backcatter [5], FreeRider [15] and MOXcatter [18], where FS-backcatter is content-agnostic system. The results, presented in Fig. 6.11a, b, demonstrate that CAB consistently outperforms the other systems. Specifically, when the tag-receiver distance is 7 m,

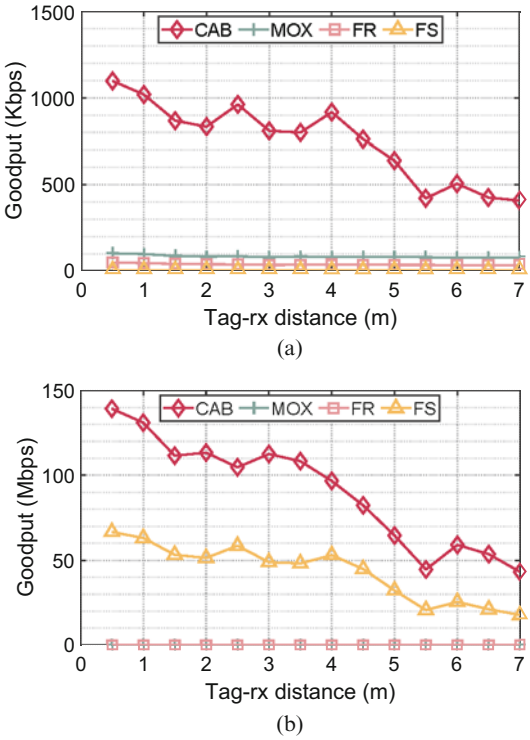


Fig. 6.11 Goodput comparison. (**a**) Goodput of tag data. (**b**) Goodput of ambient data

CAB achieves a tag-data goodput of 408.56 kbps, which surpasses the performance of MOXcatter, FreeRider, and FS-backscatter by factors of 6.7×, 12.5×, and 207.4×, respectively. The goodput gains further increase to 8.1×, 16.0×, and 269.7× when the tag-receiver distance is reduced to 1 m. These improvements can be attributed to two key factors. Firstly, our baseline systems utilize multi-symbol or packet-level modulation, whereas CAB performs backscattering on a single-symbol level, allowing for enhanced performance. Secondly, CAB supports fine-grained PSK modulation, while the baseline systems employ two-level AM modulation. Furthermore, CAB once again demonstrates its superiority in goodput of ambient data. For example, CAB achieves an ambient-data goodput of 53.59 Mbps at a tag-receiver distance of 6.5 m, outperforming FS-backscatter by a factor of 2.5×. Additionally, in our random-data setup, both FreeRider and MOXcatter achieve zero ambient-data goodput.

6.5.2.2 Micro Benchmarks

Estimating Zero-subcarrier Phases Initially, we investigate the performance of various phase-estimation schemes. In addition to WLS, we evaluate the effective-

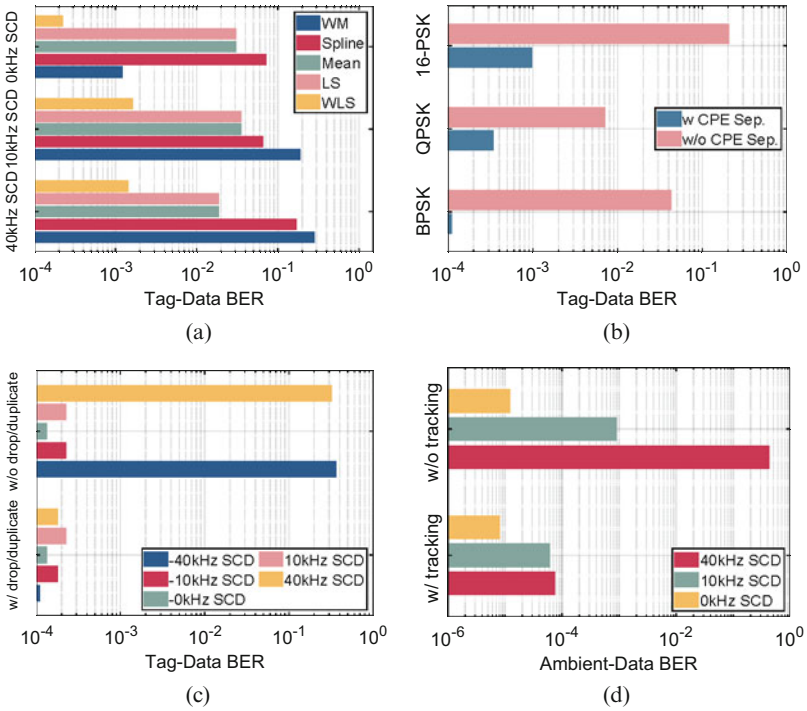


Fig. 6.12 BERs are improved by a series of operations. (**a**) Phase estimation. (**b**) CPE separation. (**c**) Symbol assembly. (**d**) Phase tracking

ness of mean (simple averaging), weighted mean, LS (Least Squares), and cubic spline interpolation techniques. For tag modulation, we employ QPSK. The results of Fig. 6.12a show that for different Sampling-Clock Differences (SCDs), the tag-data BER obtained using WLS is consistently lower than 0.16%, which indicates that WLS is superior to other methods.

Impact of CPE Separation In our subsequent investigation, we intend to assess the influence of CPE separation on the demodulation of tag data. We employ BPSK, QPSK, and 16PSK modulations for the tag, and the corresponding outcomes are depicted in Fig. 6.12b. We make two key observations from the results. Firstly, our CPE separation technique significantly enhances the accuracy of tag-data demodulation. Specifically, the tag-data BER achieves 0.011% when using CPE separation under BPSK, whereas it increases to 4.2% when no CPE separation is employed. This indicates a remarkable 383× improvement in performance. Secondly, we observe a gradual degradation with CPE separation method as the order of PSK modulation increases, which aligns with the behavior observed in active radio systems utilizing high-order modulation schemes [17]. Nevertheless, even for 16PSK modulation, the tag-data BER remains below 0.97%.

Impact of Symbol Assembly Figure 6.12c showcases the effectiveness of our precise symbol assembly in significantly reducing tag-data BERs. Notably, when the SCD is set to −40 kHz, the tag-data BER without the use of our symbol assembly is recorded at 36%; however, after implementing our symbol assembly, the BER drastically diminishes to 0.011%. Moreover, across all SCD conditions, the tag-data BERs consistently remain below 0.024%, which attests to the consistent and reliable performance of our symbol assembly technique.

Customized Phase Tracking The results presented in Fig. 6.12d demonstrate a significant reduction in ambient-data BERs. Specifically, when the SCD is set to 40 kHz, the ambient-data BER prior to phase tracking is measured at 42%. However, after applying our phase tracking methodology, the BER drastically reduces to a mere 0.01%. This remarkable improvement can be attributed to our symbol-by-symbol phase tracking process, which effectively avoids issues associated with incorrect pilot averaging and inter-symbol phase unwrapping. Additionally, across all tested SCD conditions, the ambient-data BERs consistently remain below 0.01%.

Ambient Traffic for Tag Streaming We connect a Dell laptop to an AP via Wi-Fi 4, generating typical Wi-Fi traffic in various scenarios. We initiate a download of a 10 GB file. Then, we stream a 1080p, 30fps movie online. The traffic persists throughout the duration of the file download or video playback, although with significant rate fluctuations. The battery-free prototype backscatters the camera's image data at 240p. The receiver processes the received backscattered signals in real-time, demodulating the backscattered live streams. We utilize the intra-frame algorithm presented in [36], achieving an average compression ratio of 69×. Furthermore, by employing inter-frame compression [36], we achieve an additional average compression ratio of 38×.

The streaming results are depicted in Fig. 6.13. We observe that the ambient Wi-Fi traffic generated during file downloading remains relatively stable at around 20 Mbps, while the traffic produced during video streaming exhibits fluctuations, with peaks reaching approximately 19 Mbps and lows dropping to around 2 Mbps. This variation can be attributed to the utilization of cache servers, which are commonly employed by HTTP-streaming platforms to enhance the Quality of Experience (QoE) for viewers. Additionally, we notice that the streaming traffic from the battery-free tag closely resembles the excitation traffic. For instance, when utilizing file-downloading excitations, we achieve an average tag-streaming rate of 37.1 frames per second. This result demonstrates the capability of CAB for enabling battery-free live streaming.

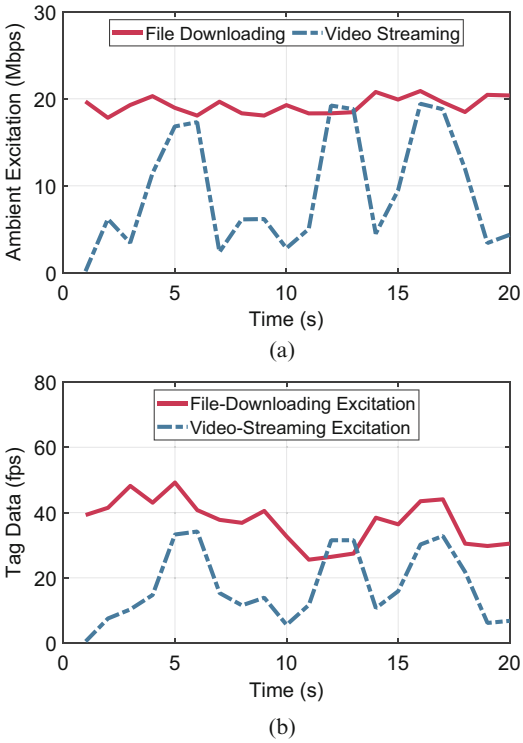


Fig. 6.13 Tag streaming with uncontrolled traffic. (**a**) Ambient traffic. (**b**) Tag streaming data

6.6 Application Case

6.6.1 Smart Agricultural

The advancement of IoT technology has heightened the significance of efficiency and intelligence in agricultural production. Traditional agriculture, due to human limitations and long distances, resorts to crude methods for planting and maintaining fruit trees. The quality and quantity of harvested fruits can be severely impacted by birds and pests. In addition, due to the lack of real-time monitoring equipment with low energy consumption and low deployment costs, farmers must conduct frequent inspections to identify existing and potential problems. This inefficient monitoring method consumes much time but cannot respond effectively to unexpected situations. Smart agriculture aims to optimize farming practices by harnessing advanced technologies. One such technology is the ambient backscatter communication system, which enables low-power, long-range wireless communication by utilizing existing ambient signals as a power source.

By employing a high-throughput backscatter system based on CAB, farmers can wirelessly and remotely operate smart agriculture applications, simplifying the monitoring and management of agricultural operations. Farmers can access

real-time data collected by sensors from their smartphones, tablets, or computers, enabling them to make well-informed decisions regarding irrigation, fertilization, pest control, and other aspects of crop management. For instance, when a large group of birds lands on a tree to nibble on mature fruits, fruit farmers can remotely activate bird-repellent noise to safeguard their agricultural achievements. Moreover, by utilizing the backscatter communication system to gather feedback on soil moisture and air temperature, farmers can promptly water fruit trees while staying informed about their real-time status. Additionally, the backscatter communication system employed in smart agriculture can integrate image recognition, cloud computing, and other information technologies to facilitate efficient processing and rapid response to the vast volume of agricultural data collected by sensors. In summary, the combination of smart agriculture and our CAB system can offer a solution for augmenting efficiency and productivity in agriculture.

6.7 Discussion and Future Work

6.7.1 COTS Receiver

Currently, a limitation of employing commodity off-the-shelf devices as receivers for CAB is the inability to access pilot subcarriers on the PHY layer using current Wi-Fi network interface controllers (NICs). Nevertheless, we have optimism regarding the future implementation of CAB in commodity NICs. This optimism arises from the increasing availability of APIs for PHY data in NICs, which allows for the incorporation of various functions. The Linux CSI Tool [37] provides a convenient means of obtaining Channel State Information (CSI) by utilizing modified firmware, providing output from 30 selective data subcarriers. Moreover, Bluetooth 5 direction-finding packets include CTE (Constant Tone Extension) fields that transmit IQ data to the receiver host. This functionality allows for channel analysis and transmitter localization [38]. These developments suggest that the integration of CAB into commodity NICs is a feasible future direction.

6.7.2 Ambient Traffic Patterns

While CAB is designed to work with different ambient traffic patterns, the accuracy of its ambient-data demodulation could degrade in the presence of sporadic Wi-Fi traffic due to the instability of the intervals between packets, which affects synchronization. However, this does not significantly affect tag-data demodulation. As a future direction, we plan to develop low-power Wi-Fi demodulation schemes that can extract S-LTF and L-LTF fields in order to address this limitation.

6.7.3 QAM Modulation

To boost the throughput of tag data, higher-order modulation schemes are critical since they allow more bits to be transmitted in a single symbol. Nevertheless, the implementation of these schemes requires improvements to the current tag modulation scheme and the development of QAM modulation circuits for backscattering. These enhancements are necessary to guarantee the efficient and fast transmission of tag data.

6.8 Summary

In this chapter, we present CAB, a content-agnostic ambient Wi-Fi backscatter system capable of demodulating both tag and ambient data solely from backscattered signals. The primary innovation of our approach lies in utilizing zero-subcarriers. This design is based on our insight that uncontrolled OFDM Wi-Fi signals can be treated as virtual single tones. We also present how CAB handles various Wi-Fi excitations using customized demodulation methods. Our system represents a significant advancement towards enabling ubiquitous battery-free IoTs, and it serves as a catalyst for the rapid and widespread adoption of pervasive ambient backscatter communication. We firmly believe that this development marks a crucial step forward in the field.

In this part, we present four advanced works that can effectively use the ambient Wi-Fi signal for efficient data transmission. We are constantly trying to reduce the granularity of modulation to improve the throughput rate of the system, and innovating modulation methods to reduce the cost of the system. In the next part, we will further explore multi-hop, multi-source backscatter systems and lay the foundation for a network of backscatter systems.

References

1. Wang J, Hassanieh H, Katabi D, Indyk P. (2012) Efficient and reliable low-power backscatter networks. In: Proceedings of ACM SIGCOMM
2. Liu V, Parks A, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. In: Proceedings of ACM SIGCOMM
3. Talla V, Kellogg B, Ransford B, Naderiparizi S, Gollakota S, Smith JR (2015) Powering the next billion devices with wi-fi. In: Proceedings of ACM CONEXT
4. Jang J, Adib F (2019) Underwater backscatter networking. In: Proceedings of ACM SIGCOMM
5. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of ACM SIGCOMM
6. Zhang M, Chen S, Zhao J, Gong W (2021) Commodity-level BLE backscatter. In: Proceedings of ACM MobiSys

7. Zhao J, Gong W, Liu J (2020) Towards scalable backscatter sensor mesh with decodable relay and distributed excitation. In: Proceedings of ACM MobiSys
8. Abdelhamid MR, Chen R, Cho J, Chandrakasan AP, Adib F (2020) Self-reconfigurable micro-implants for cross-tissue wireless and batteryless connectivity. In: Proceedings of ACM MobiCom
9. Ma Y, Luo Z, Steiger C, Traverso G, Adib F (2018) Enabling deep-tissue networking for miniature medical devices. In: Proceedings of ACM SIGCOMM
10. Mazaheri MH, Chen A, Abari O (2021) MMTAG: a millimeter wave backscatter network. In: Proceedings of ACM SIGCOMM
11. Chi Z, Liu X, Wang W, Yao Y, Zhu T (2020) Leveraging ambient LTE traffic for ubiquitous passive communication. In: Proceedings of ACM SIGCOMM
12. Liu X, Chi Z, Wang W, Yao Y, Hao P, Zhu T (2021) Verification and redesign of OFDM backscatter. In: Proceedings of USENIX NSDI
13. Kellogg B, Parks A, Gollakota S, Smith JR, Wetherall D (2014) Wi-fi backscatter: internet connectivity for RF-powered devices. In: Proceedings of ACM SIGCOMM
14. Wang Q, Chen S, Zhao J, Gong W (2021) Rapidrider: efficient wifi backscatter with uncontrolled ambient signals. In: Proceedings of IEEE INFOCOM
15. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of ACM CONEXT
16. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of ACM SenSys
17. Tse D, Viswanath P (2005) Fundamentals of wireless communication. Cambridge University Press, Cambridge
18. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of ACM MobiSys
19. Zhao J, Gong W, Liu J (2018) X-tandem: towards multi-hop backscatter communication with commodity wifi. In: Proceedings of ACM MobiCom
20. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) Plora: a passive long-range data network from ambient lora transmissions. In: Proceedings of ACM SIGCOMM
21. Yang Y, Yuan L, Zhao J, Gong W (2022) Content-agnostic backscatter from thin air. In: Proceedings of ACM MobiSys
22. 802.11a. https://standards.ieee.org/standard/802_11a-1999.html
23. 802.11g. https://standards.ieee.org/standard/802_11g-2003.html
24. 802.11n. https://standards.ieee.org/standard/802_11n-2009.html
25. 802.11ac. https://standards.ieee.org/standard/802_11ac-2013.html
26. 802.11ax. https://standards.ieee.org/standard/802_11ax-2021.html
27. Rahul H, Hassanieh H, Katabi D (2020) Sourcesync: a distributed wireless architecture for exploiting sender diversity. In: Proceedings of ACM SIGCOMM
28. Vasisht D, Kumar S, Katabi D (2016) Decimeter-level localization with a single wifi access point. In: Proceedings of USENIX NSDI
29. Speth M, Fechtel SA, Fock G, Meyr H (1999) Optimum receiver design for wireless broadband systems using OFDM. I. IEEE Trans Commun 47(11):1668–1677
30. Tan JK (2006) An adaptive orthogonal frequency division multiplexing baseband modem for wideband wireless channels. PhD Thesis, Master's thesis, MIT
31. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In: Proceedings of ACM SIGCOMM
32. ZedBoard. https://digilent.com/reference/_media/zedboard:zedboard_ug.pdf
33. FMCOMMS3. https://wiki.analog.com/resources/eval/user-guides/ad-fmcomms3-ebz
34. Kamalinejad P, Keikhosravy K, Molavi R, Mirabbasi S, Leung VCM (2014) An ultra-low-power CMOS voltage-controlled ring oscillator for passive RFID tags. In: Proceedings of IEEE NEWCAS

35. Lee KK, Granhaug K, Andersen N (2014) A study of low-power crystal oscillator design. In: Proceedings of IEEE NORCHIP
36. Naderiparizi S, Hessar M, Talla V, Gollakota S, Smith JR (2018) Towards battery-free hd video streaming. In: Proceedings of USENIX NSDI
37. CSI Tool. https://dhalperi.github.io/linux-80211n-csitool/
38. Bluetooth. https://www.bluetooth.com/specifications/bluetooth-core-specification/

Part III
Towards Backscatter Networks at Scale

Part III includes several of the most advanced ambient backscatter network solutions, which are made possible by the first multi-hop backscatter (Chap. 7), first backscatter mesh (Chap. 8), and multiprotocol backscatter (Chap. 9).

Chapter 7
Multi-Hop Wi-Fi Backscatter

Abstract From Chaps. 3–6, we have presented multiple backscatter systems working with ambient signals such as Wi-Fi. However, all of them work in a single-hop mode without any intermediate relaying, which leads to limited connectivity when the channel is unreliable, thereby falling short of the Internet-of-Things (IoT) vision for ubiquitous communication. Therefore, in this chapter, we introduce a novel multi-hop backscatter communication system compatible with off-the-shelf Wi-Fi devices, namely X-Tandem. We demonstrate that the tags can serve as relays while modulating their sensing data into the same backscatter packet. This backscattered packet is still a valid Wi-Fi packet, which can be decoded using off-the-shelf Wi-Fi devices. In particular, we first introduce the motivation for employing multi-hop backscatter communication. Then, a fundamental background involving the Wi-Fi physical layer is presented. After that, we discuss our system design in detail. Next, an extensive performance evaluation is given. We also present several potential application cases driven by our multi-hop backscatter system. Finally, we summarize and discuss our work.

7.1 Introduction

7.1.1 Motivation and Background

As we discussed in Part I, ambient backscatter communication (Amb-BackCom) has the ability to provide a cost-efficient and energy-efficient means to exchange Internet-of-Things (IoT) sensor data. Recent studies in [1–13] have demonstrated such abilities from various angles. However, a crucial fact is that all these schemes work in a single-hop mode, i.e., there is only one direct communication link between the tag and the receiver, which causes limited connectivity when the channel becomes unreliable, thereby severely limiting the resilience and scalability of Amb-BackCom, ultimately failing to fulfill the IoT goal of ubiquitous interconnection. As such, we naturally ask: *how can we resolve those issues?*

Let us look back to conventional network design, in which essential issues like robustness, throughput, and scalability are efficiently addressed by constructing end-

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_7

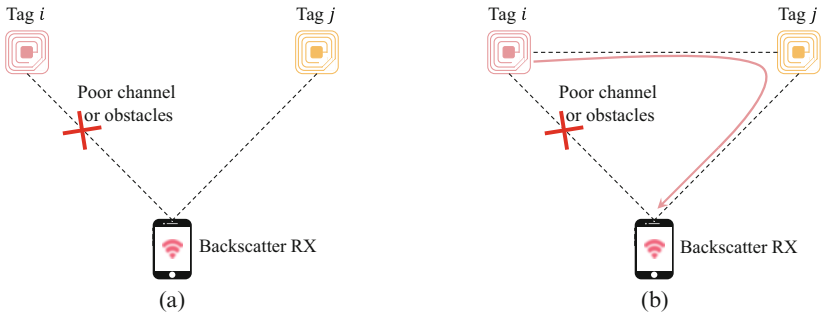


Fig. 7.1 A comparison between single-hop backscatter and multi-hop backscatter: multi-hop backscatter enables robustness and path diversity compared to single-hop backscatter. (**a**) Single-hop backscatter. (**b**) Multi-hop backscatter

to-end path diversity. The multipath transmission in datacenters networks [14, 15] and the datapath adaptation in multi-hop wireless sensor networks [16, 17] are two typical examples. Therefore, we spontaneously ask the following questions: *can Amb-BackCom benefit from path diversity? Furthermore, can we build a multi-hop backscatter system?* Figure 7.1 presents a comparison of single-hop backscatter with multi-hop backscatter. Owing to the poor channel or obstacles, the direct communication link between the tag i and the backscatter RX (i.e., receiver) is inaccessible. As a result, the single-hop backscatter receiver is unable to receive Tag i's data. Conversely, in the same scenario, the multi-hop backscatter can leverage Tag j's relay as an alternative path. Our experimental results in Sect. 7.5.2 indicate that tag relay is effective in addressing unreliable communication channels, particularly in cases where densely deployed tags are obstructed by physical obstacles such as people in motion, walls, or indoor structures.

Motivated by the aforementioned observations, in this chapter, we introduce a multi-hop backscatter system. Its primary operations are depicted in Fig. 7.2. Assuming that there exists an uninterrupted Wi-Fi signal, the first-hop tag utilizes this signal as an excitation and embeds its sensing data onto it. Subsequently, the second-hop tag receives the reflected signal from the first-hop tag and then forwards the first-hop tag's data while modulating its data onto the same backscattered signal. Finally, two commodity Wi-Fi devices are used to decode the data from multi-hop tags by comparing the backscattered Wi-Fi signal with the original Wi-Fi signal.

7.1.2 Challenges

To implement such a multi-hop backscatter system depicted in Fig. 7.2, however, we encounter a series of challenges.

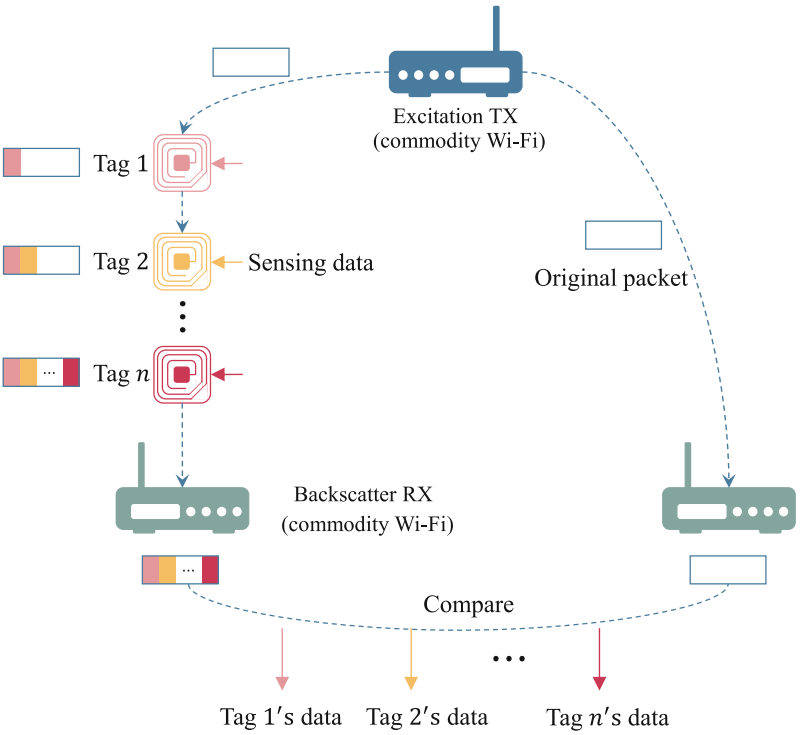


Fig. 7.2 The overview of multi-hop backscatter communication. Each tag relays for previous hops while embedding its sensing data on the original Wi-Fi signals, fully working with off-the-shelf Wi-Fi devices

1. The multi-hop backscatter paradigm depicted in Fig. 7.2 follows an in-order route (i.e, Tag 1 →Tag 2 → ⋯ →Tag n →backscatter receiver). In comparison with the single-hop (i.e., tag-to-receiver) mode, this multi-hop mode produces a succession of intermediate backscattered signals, thereby probably involving additional decoding operations. Due to the spread of those signals across Wi-Fi frequencies, moreover, our system faces both the interference between the original signal and the reflected signal, and the interference among multiple relays.
2. Modulating multi-hop tag data into the same packet involves various configuration operations on the tag hardware. These operations include route allocation and the synchronization of multiple tag data with specific data fields. To ensure these operations are carried out successfully, an efficient control mechanism is necessary, preferably without the need for additional decoding operations.
3. Given an example of the two-tag scenario, in the ideal case, multi-hop tag modulation should follow the following route: 1st-hop tag → 2nd-hop tag → receiver. However, some packets may be initially backscattered by the second-hop tag, and subsequently by the first-hop tag, as illustrated in Fig. 7.3. As such,

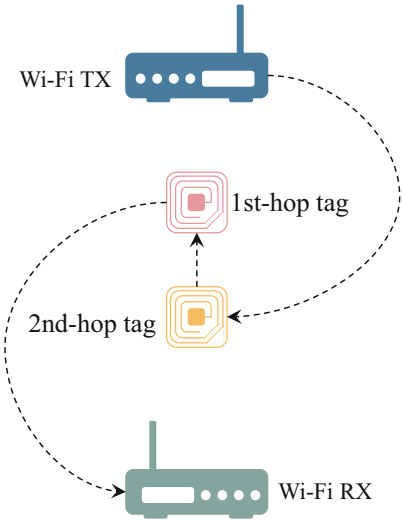


Fig. 7.3 Out-of-order tags

the out-of-order reflection occurs. The situation gets worse especially when the tags are near each other, thereby probably causing a significantly negative impact during decoding.

7.1.3 Solutions

Our solutions are summarized as follows.

- We design a novel Multiple Frequency Shifts (MFS) scheme to enable signal relay among multiple tags. Using this scheme, an original Wi-Fi signal to be backscattered more times, with each backscatter operation shifting the backscattered signal frequency band far away from the incoming signal frequency band, thereby eliminating the interference between the original signal and the reflected signals, as well as the interference among multiple relays.
- We propose a smart data field allocation scheme to coordinate the transmission from multi-hop tags. In particular, the order of tags for backscattering is specified by using control signals, and each tag is assigned to a different packet's data fields.
- We present a novel packet verification scheme that is able to filter out-of-order backscattered packets. Our key insight is that there is a large difference in the packet received signal strength indicator (RSSI) of out-of-order backscattered packets and in-order backscattered packets. Thus, by setting an appropriate threshold, we can separate the two types of packets.

In our multi-hop backscatter communication system, the tag relay adopts analog forwarding, which means that a tag does not need to decode the incoming data from other tags. In comparison with digital forwarding where a tag needs to decode the backscattered signals from other tags, our solution not only reduces hardware complexity but also is able to perform tag modulation and tag relay at the same time. To verify the effectiveness of our design, we prototype our multi-hop backscatter system using FPGAs and off-the-shelf Wi-Fi devices, and evaluate the performance of our system in different scenarios. The experiment results demonstrate that our multi-hop design has a substantial positive impact on the backscatter range and communication quality, particularly when faced with obstacles.

7.2 Related Work

In this chapter, we introduce a multi-hop backscatter system compatible with off-the-shelf Wi-Fi devices. Our multi-hop backscatter design is inspired by the recent studies in [18–26], which are discussed as follows.

Wi-Fi Backscatter The first Wi-Fi-based backscatter system is introduced by Kellogg et al. in [18], which achieves the communication between tags and commodity Wi-Fi devices. Since then, there is a growing interest in the design of backscatter systems compatible with off-the-shelf Wi-Fi radios. BackFi [19] presents a novel backscatter tag to work with existing Wi-Fi signals. Passive Wi-Fi [20] reduces the power consumption of Wi-Fi transmissions by using a novel backscatter tag infrastructure. Inter-Technology Backscatter [21] achieves the backscatter communication between Bluetooth and Wi-Fi. FS-Backscatter [22] proposes a novel frequency-shifting technique to eliminate the interference between the incoming and backscattered signals. HitchHike [23] introduces a novel modulation approach called codeword translation to enable the backscatter system completely compatible with off-the-shelf 802.11b Wi-Fi devices. FreeRider [24] extends the codeword translation approach to commodity ZigBee, Bluetooth, and 802.11g/n Wi-Fi radios. Nevertheless, these studies operate in a single-hop mode (i.e., transmission from a tag to a receiver). Different from these single-hop backscatter systems, [26] builds a multi-hop backscatter communication system (i.e., transmission from tag i to $\cdots$ to tag j to a receiver).

Relay Forwarding Relay forwarding is an efficient solution to extend the communication range. Ma et al. propose RFly [25], a backscatter system that uses the drone as the relay device between the tag and the receiver. In this system, RFly drones can forward a query from a backscatter receiver to a tag or transmit the response from the tag to the backscatter receiver. The experimental results demonstrate that RFly can achieve a communication range of over 50 m. Although our multi-hop backscatter system also supports relay forwarding, it is essentially different from RFly [25] in three aspects: (i) RFly adds an additional drone to the existing backscatter system to enable relay forwarding, while our system itself is able to perform relay forwarding

without the need for any external devices; (ii) In RFly, the drone does not generate any data by itself when relaying information, while our tag transmits its data and performs relays at the same time; (iii) RFly operates with RFID infrastructures, while our system works with off-the-shelf Wi-Fi radios.

7.3 Wi-Fi PHY Primer

In this section, we provide an overview of the Wi-Fi transmitter's system architecture [27–30], which is an important preliminary for understanding Sect. 7.4.2.3. As depicted in Fig. 7.4, a Wi-Fi transmitter consists of two primary systems: (i) system A and (ii) system B.

- *System A*: Through System A, the incoming data bit stream is mapped into the I/Q data in the constellation. For different Wi-Fi protocols, System A involves different operations. In terms of 802.11b, System A involves barker coding, scrambling, and constellation mapping, while in 802.11g, System A involves convolutional encoding, scrambling, constellation mapping, and interleaving. In both cases, System A is linear over the position and value of the original data bit. In advanced Wi-Fi standards such as 802.11n, however, spatial multiplexing has been introduced, and System A includes a spatial stream parser. This steam parser distributes successive data bits to multiple spatial streams in a round-robin fashion, thereby leading to non-linear System A. In Sect. 7.4.2.3, we will observe that our multi-hop backscatter system supports four different types of phase modulation when System A is linear. However, if System A is non-linear, only two types of phase modulation can be supported.
- *System B*: It utilizes the I/Q data outputted from System A to produce RF signals. System B involves several operations such as Inverse Discrete Fourier Transform (IDFT) for OFDM. System B is linear over the I/Q data space, indicating that a phase shift in the time-domain waveform results in a corresponding phase shift in the I/Q constellation points.

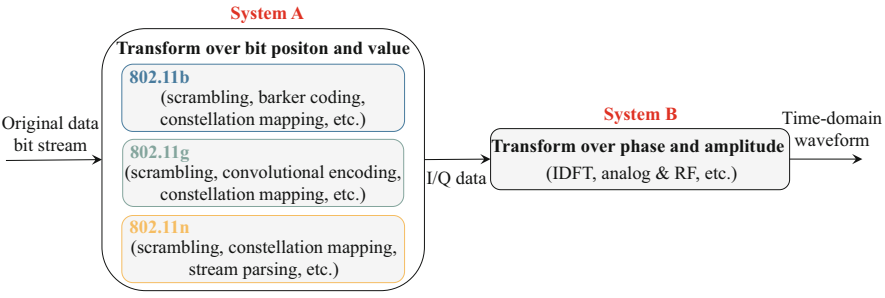


Fig. 7.4 The overview of Wi-Fi transmitter

7.4 System Design

This section provides an elaborate exposition of system design, as shown in Fig. 7.5. The transmitter first produces the control signals, which carry important commands indicating route allocation and data fields allocation for multiple tags. Once the tag relay is activated, the tag will try to identify protocols and packet length, and then compute the number of bits embedded in a packet. Subsequently, the tag leverages the codebook translation technique to modulate and reflect the incoming signal to transmit its sensing data. To avoid interference, each tag shifts the incoming signal into another frequency band. Finally, two commodity Wi-Fi receivers are used to decode the data from multiple tags, in which only the original signal and last-hop backscattered signal are utilized.

7.4.1 Transmitter Side

Control Signals Generation For the sake of simplicity, we present a two-tag scenario as an example to illustrate how to generate control signals. Assuming that the IDs of the two tags are '01' and '10', there are four types of control signals: (i) six long-duration packets implying that the tag relay switches on; (ii) six short-duration packets implying that the tag relay switches off; (iii) three long-duration packets followed by three short-duration packets implying that the ID of the first-hop tag is'01'; (iv) three short-duration packets followed by three long-duration packets implying that the ID of the first-hop tag is '10', as shown in Fig. 7.6. The long-duration packet and the short-duration packet are respectively generated by using 802.11b 1Mbps mode and 802.11n Doule Streams (DS) 13Mbps mode to send a packet with a 2024 Bytes payload.

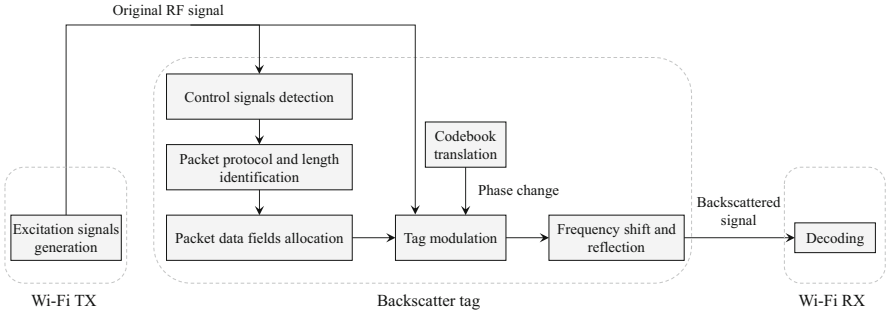


Fig. 7.5 The overview of system design

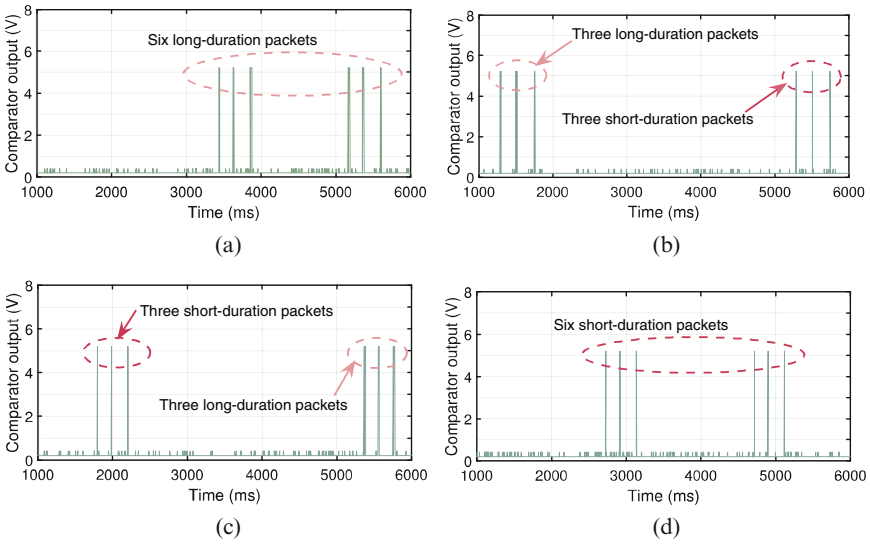


Fig. 7.6 The four different types of control signals. (**a**) Tag relay on. (**b**) First hop: tag '01'. (**c**) First hop: tag '10'. (**d**) Tag relay off

7.4.2 Tag Side

As shown in Fig. 7.5, the backscatter tag performs the following operations, including control signals detection, packet protocol and length identification, packet data fields allocation, tag modulation, and frequency shift, which we discuss in the following Subsections.

7.4.2.1 Control Signals Detection

The control signals detection module mainly consists of three blocks, as shown in Fig. 7.7. Each block contains a counter and a comparator for digital values. The first block serves to identify a short or long packet based on its duration. The following two blocks compute the number of long-duration and short-duration packets, respectively. As such, the tag can take a corresponding action, such as switching on its relay.

7.4.2.2 Packet Protocol and Length Identification

Following the control signals, the tag will receive the predefined packets that contain fixed payload data bits. These packets serve the purpose of identifying protocols and determining the modulation range assigned to each tag. Our key insight is that

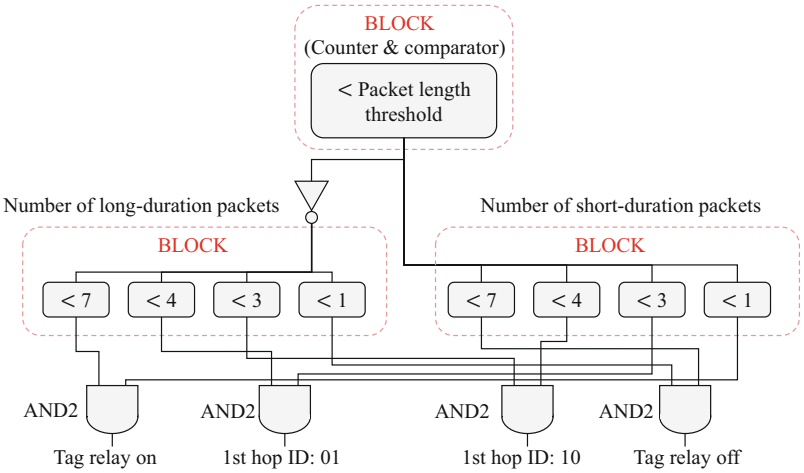


Fig. 7.7 The module of detecting control signal

when sending an equivalent amount of data, different protocols display different durations. Consequently, if the tag can measure the duration of the signal, it will identify the protocol type. To accomplish this, the tag employs an RF power detector composed of a 50 Ω impedance matching network, a multi-stage power amplifier, a summation, and a low pass filter, as shown in Fig. 7.8. The detector can transform the incoming RF signal into a corresponding DC voltage, as illustrated in Fig. 7.9a. We can observe that the basic signal characteristics, including the signal's start time, end time, and duration, can be captured. Next, we use a voltage comparator to filter the noise voltage in Fig. 7.9a. This comparator output is depicted in Fig. 7.9b. By directing the comparator output to the FPGA and utilizing a counter with clock frequency, we can obtain the packet duration, thereby identifying protocols and packet length.

7.4.2.3 Multi-Hop Tag Modulation in a Packet

In our system, tag modulation leverages the codeword translation approach proposed in [23]. This approach has been conducted and evaluated in various backscatter systems, including Wi-Fi 802.11b [23], 802.11g/n OFDM, ZigBee [24], Bluetooth, and 802.11n MIMO-OFDM double streams [10]. The codeword translation changes the phase of the original data while making the phase of the backscattered data remain within the same constellation, as illustrated in Fig. 7.10. Therefore, for commodity radios, such as Wi-Fi, this means that an off-the-shelf Wi-Fi device can decode the backscattered signal.

To provide a better understanding of why phase changes can maintain data within the same constellation, we utilize the Wi-Fi transmitter depicted in Fig. 7.4 as an

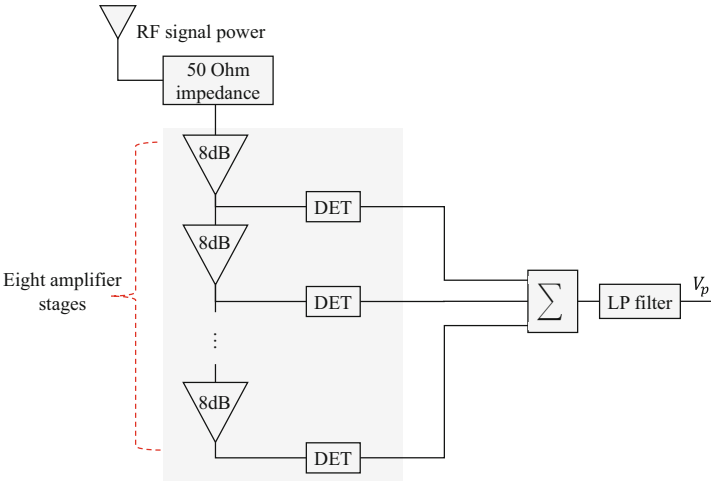


Fig. 7.8 The RF power detector

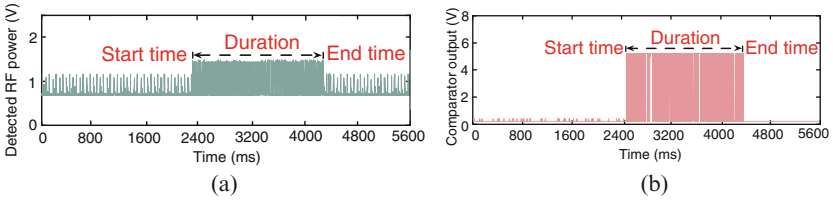


Fig. 7.9 (**a**) The RF power detector output. (**b**) The voltage comparator output. Here, the signal type used is 802.11n and the size of the payload data transmitted is 1.06M bytes

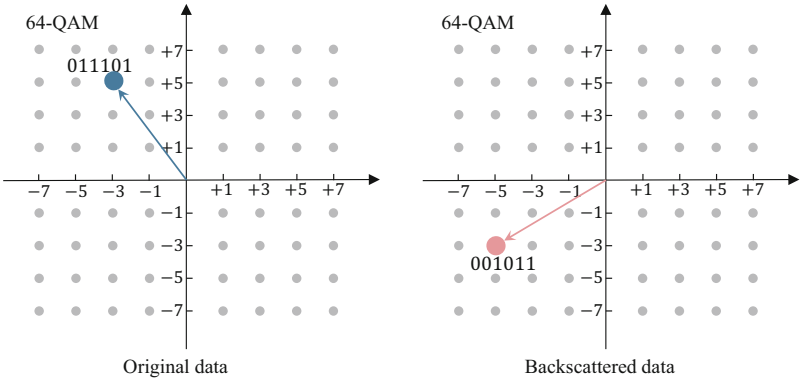


Fig. 7.10 The backscattered data remains within the 64-QAM constellation when tag modulation introduces a 90° of phase shift

example. In the case of 802.11b/g and 802.11n single-stream, System A and System B in Fig. 7.4 can be viewed as linear transformations in phase. We define $\mathbb{H}$ as a transform containing all the operations, such as scrambling and encoding. We denote the original data and the time-domain signal carrying the original data as $Y(t)$ and X, respectively. Thus, we obain $Y(t) = \mathbb{H}(X)$. Next, the tag introduces a phase change (denoted by θ) operation on $Y(t)$. The tag modulation operation can be expressed as follows:

$$\theta \cdot Y(t) = \theta \cdot \mathbb{H}(X) = \mathbb{H}(\theta \cdot X) \tag{7.1}$$

When the receiver performs inverse operations $\mathbb{H}^{-1}$, the backscattered data can be expressed as θX. By selecting an appropriate phase change, it is possible for θX to fall within the same constellation. Regarding 802.11n multi-stream, however, the transmitter employs a stream parser, which results in a non-linear transform of phase change, as discussed in Sect. 7.3. But we find that phase changes of 0° or 180° still work.

On the basis of the modulation method mentioned above, two approaches can be utilized to modulate multi-hop tag data into one packet. The first is to let each tag individually change the phase of the same packet data fields. The other is to divide the data fields into pieces and assign them to different tags. Although the former allows each tag to embed more data bits, it requires the backscattered signal from every hop for decoding, and tags are mutually dependent on modulation. Conversely, the latter only requires the backscattered signal from the last hop, and the tags are independent of each other. Therefore, we select the latter and introduce the following packet data fields allocation scheme.

7.4.2.4 Packet Data Fields Allocation Among Tags

In general, a Wi-Fi packet includes the header field and the data field (i.e., the payload field). The header field carries some critical information for synchronization. Therefore, we choose the payload field to carry multiple tags' data. Figure 7.11 presents the example of an 802.11n packet's data field allocation, in which each tag is assigned to a specific part of data fields, following the order of hops. We define D_{packet}, $D_{preamble}$, D_{header}, and D_{data} as the packet duration, preamble duration, MAC header duration, and data fields' duration, respectively. Thus, D_{data} can be computed as follows:

$$D_{data} = D_{packet} - D_{preamble} - D_{header} \tag{7.2}$$

where D_{packet} can be obtained based on Sect. 7.4.2.2; $D_{preamble}$ and D_{header} are constant given a Wi-Fi protocol. To avoid interference among backscattered signals, we introduce the separating fields. We denote the total duration of the separating

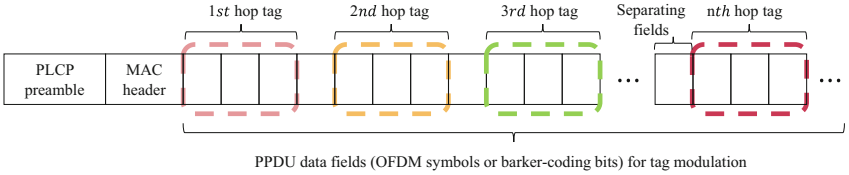


Fig. 7.11 An example showing an 802.11n packet's data field allocation

fields as D_s. Therefore, the number of OFDM symbols assigned to each tag, denoted by N^{OFDM} can be calculated as follows:

$$N^{OFDM} = \left\lfloor \frac{D_{data} - D_s}{m \cdot T_{sym}} \right\rfloor \tag{7.3}$$

where T_{sym} and m denote the symbol duration and the number of tags, respectively. Assuming that the ith tag leverages n_i OFDM symbols to modulate one-bit tag data, the number of bits that the ith hop tag data can embed in a packet, denoted by N_i^{tag}, can be formulated as follows:

$$N_i^{tag} = \left\lfloor \frac{N^{OFDM}}{n_i} \right\rfloor \tag{7.4}$$

7.4.2.5 Tag Relay by Multiple Frequency Shifts

To enable multi-hop tags relay, we design a novel Multiple Frequency Shifts (MFS) approach, in which the first hop tag performs the backscattering operation by using a square signal to multiply the original excitation signal and the ith hop tag relays the $i-1$th hop tag's reflected signal by using another wave signal to multiply it. Using this scheme, an original Wi-Fi packet can be repeatedly backscattered, with each backscatter operation shifting the reflected signal frequency band away from the incoming signal frequency band, thereby eliminating the interference between the original signal and the reflected signals, as well as the interference among multiple relays. Without loss of generality, we present a two-hop scenario as an example and use the following denotation:

- f_c: the center frequency of the excitation signal;
- $\omega_c = 2\pi f_c$;
- f_i: the square wave frequency of the ith hop tag;
- $\omega_i = 2\pi f_i$;
- $M_{tag}^i(t) = \frac{4}{\pi} \sum_{k=1}^{\infty} \frac{sin((2k-1)\omega_i t)}{2k-1}$: the square wave signals utilized by the ith hop tag;
- $S_{base}(t)$: the baseband waveform of the excitation signal;

- $R(t)$: the multi-hop backscattered signal.

Therefore, two frequency shits can be expressed as follows:

$$\begin{aligned} R(t) &= S_{base}(t)sin(\omega_c t)M^1_{tag}(t)M^2_{tag}(t) \\ &= \frac{4}{\pi^2}S_{base}(t)\Big\{\sum_{k=1}^{\infty}\sum_{l=1}^{\infty}\frac{1}{(2k-1)(2l-1)} \\ &\cdot\{sin((\omega_c-(2l-1)\omega_1+(2k-1)\omega_2)t) \\ &-sin((\omega_c-(2l-1)\omega_1-(2k-1)\omega_2)t)\} \\ &-\sum_{k=1}^{\infty}\sum_{l=1}^{\infty}\frac{1}{(2k-1)(2l-1)}\cdot\{sin(\omega_c+(2l-1)\omega_1+(2k-1)\omega_2)t \\ &-sin((\omega_c+(2l-1)\omega_1-(2k-1)\omega_2)t)\}\Big\} \end{aligned} \tag{7.5}$$

Given that $l=1$ and $k=1$, Eq. 7.5 can be rewritten as follows.

$$\begin{aligned} R(t) &= S_{base}(t)sin(\omega_c t)M^1_{tag}(t)M^2_{tag}(t) \\ &= \frac{4}{\pi^2}S_{base}(t)\Big\{sin((\omega_c-\omega_1+\omega_2)t)-sin((\omega_c-\omega_1-\omega_2)t) \\ &\quad -sin((\omega_c+\omega_1+\omega_2)t)+sin((\omega_c+\omega_1-\omega_2)t)\Big\} \end{aligned} \tag{7.6}$$

We define $\mathbb{S}_{base}$ and $\mathbb{R}(\omega)$ as the Fourier transforms of $S_{base}(t)$ and $R(t)$, respectively. Therefore, when the two tags use the same frequency shift, we obtain

$$\begin{aligned} \mathbb{R}(\omega) = \frac{2j}{\pi^2}\Big\{&2\mathbb{S}_{base}(\omega+\omega_c)-2\mathbb{S}_{base}(\omega-\omega_c)-\mathbb{S}_{base}(\omega+\omega_c-2\omega_t) \\ &+\mathbb{S}_{base}(\omega-\omega_c+2\omega_t)-\mathbb{S}_{base}(\omega+\omega_c+2\omega_t)+\mathbb{S}_{base}(\omega-\omega_c-2\omega_t)\Big\} \end{aligned} \tag{7.7}$$

From Eq. 7.7, we observe that the reflected signal of the last-hop tag is received at the frequency band $|\mathbb{R}(\omega-\omega_c-2\omega_t)|$. Such an observation is demonstrated in Fig. 7.12.

7.4.3 Receiver Side

Tag Data Decoding As discussed in Sect. 7.1.2, the receiver will receive two types of backscattered packets: (i) in-order backscattered packets and (ii) out-of-order backscattered packets. To filter these out-of-order backscattered packets, we design

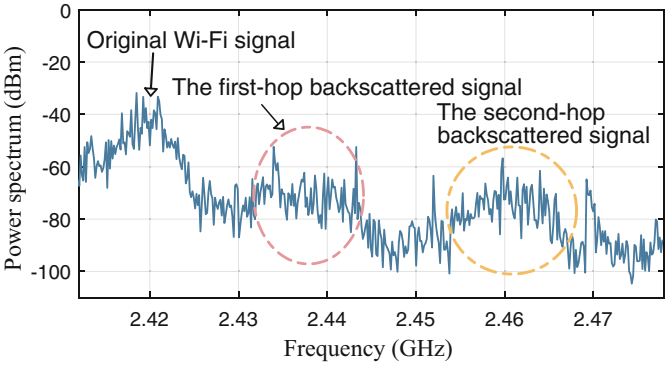


Fig. 7.12 The power spectrum of the two-hop backscattered signal over the 2.4 GHz frequency band, in which each tag employs a 25 MHz frequency shift, thereby resulting in the original Wi-Fi signal being backscattered from Channel 2 with a central frequency of 2.417 GHz to Channel 12 with a central frequency of 2.467 GHz. Decoding is implemented using only the backscattered signal from the last hop

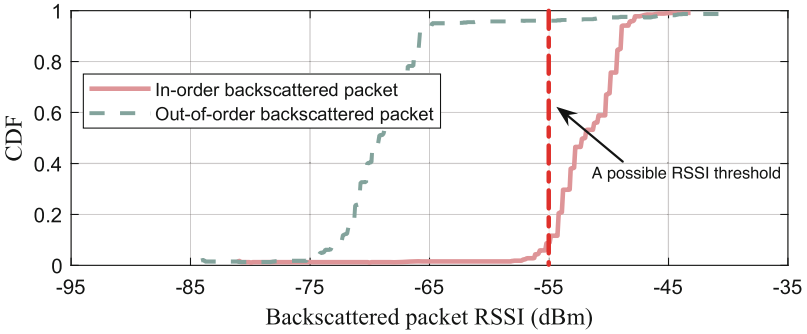


Fig. 7.13 The backscattered packet's RSSI information from in-order tags and out-of-order tags

a packet verification scheme. The key idea behind this scheme is to leverage the RSSI difference between two types of packets. Figure 7.13 show RSSI information between two types of backscattered packets. We can see that there exists a significant RSSI difference between the in-order reflected packet and the out-of-order reflected packet. This means that most of the out-of-order reflected packets can be filtered by setting an appropriate RSSI threshold.

After performing the packet verification scheme above, we utilize the XOR operation decoder proposed in [23] to decode multi-tag data. For 802.11g/n, an additional operation is performed to search the tag data from the OFDM symbols, which employs an all-zero (or all-one) sequence searching algorithm proposed in [10]. Figure 7.14 illustrates the two operations.

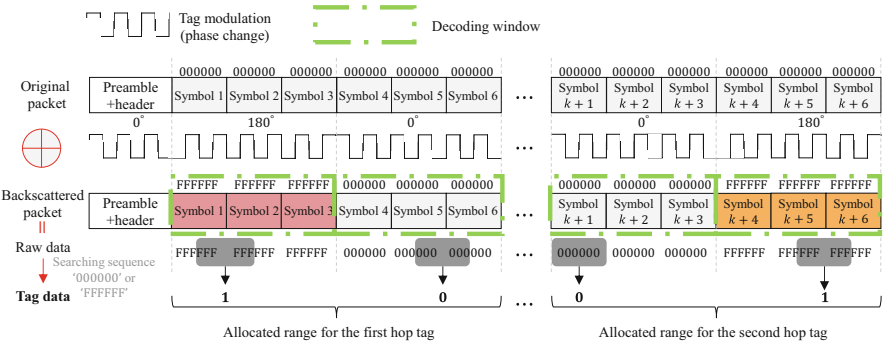


Fig. 7.14 Decoding both tags data from a backscattered packet

7.5 Performance Evaluation

7.5.1 Implementation Details

We build a prototype of our multi-hop backscatter system using FPGAs and off-the-shelf Wi-Fi devices. The implementation details are as follows.

- **Wi-Fi transceiver.** We use Dell OptiPlex 7010 equipped with Qualcomm Atheros AR938x wireless network adapter as our Wi-Fi TX/RX devices. The CommView for Wi-Fi,[1] which is a software tool that generates, receives, and analyzes 802.11 a/b/g/n/ac wireless network packets, is used to act as our Wi-Fi traffic generator. On the receiver side, the CommView for Wi-Fi is configured to operate in single-channel scanning mode and to scan channel 12 with a central frequency of 2.467 GHz. This is because we send the excitation signal from channel 2 with a central frequency of 2.417 GHz and both tags have a frequency shift of 25 MHz.
- **Tags.** Our tag prototype mainly includes the following modules:
  - *Fronted analog circuits:* Tag's fronted analog circuits consist of two main modules: (i) an RF signal power detector and (ii) a voltage comparator. These circuits are constructed using periphery components and off-the-shelf ICs. In particular, the RF power detector is implemented using AD8313, which is a multistate demodulating logarithmic amplifier with the ability to transform an RF signal into a corresponding DC voltage. The voltage comparator is implemented using TLV3510, which is a threshold voltage tuning circuit.
  - *Control signal detection and data fields allocation circuits:* These circuits are implemented by XILINX Spartan XC3S500E-4PQ208 FPGAs.

[1] http://www.tamos.com/products/commwifi/.

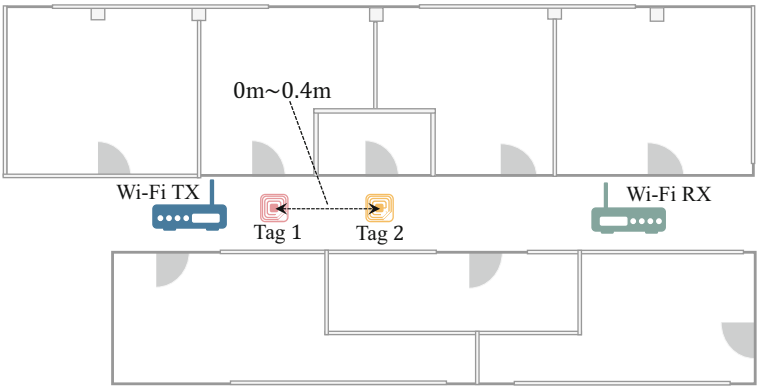


Fig. 7.15 The indoor scenario

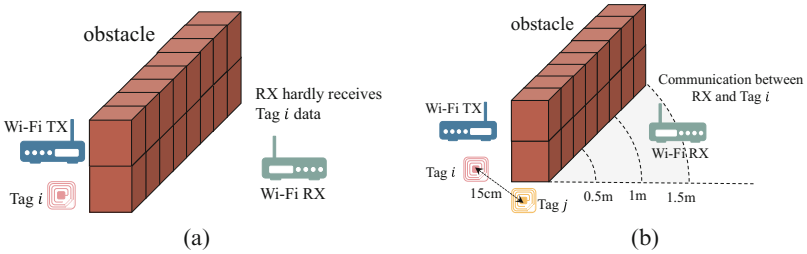


Fig. 7.16 The scenario of using tag relay. (**a**) No tag relay. (**b**) Tag relay

  - *Tag modulation circuits:* The tag modulation module mainly contains a square waveform generation circuit, a 4-input multiplexer, and an RF switch. The 4-input multiplexer is employed to choose between the four different phases 0°, 90°, 180°, and 270°, and its output is utilized to control the RF switch. The square wave generation circuit is constructed using a XILINX FPGA's Digital Clock Manager (DCM) IP core. The RF switch uses ADG902.

- **Experiment setup.** Our experiments are conducted in different scenarios, including (i) an 33 × 15 m indoor area with line-of-sight and non-line-of-sight cases, as shown in Fig. 7.15, to evaluate the effect of varying tag-to-RX and tag-to-tag distances on the two-hop reflected signal strength, throughput, and bit error rate; (ii) an obstacle experiment scenario, as shown in Fig. 7.16, to examine the impact of tag relay on performance in the presence of obstacles between a single-hop tag and a backscattered receiver.

7.5.2 Experimental Results

7.5.2.1 Communication Ranges

In terms of communication ranges, our system is evaluated using the scenario depicted in Fig. 7.15. As discussed in Sect. 7.4.2.2, our tag is able to identify different Wi-Fi protocols. Thus, we test three different types of Wi-Fi signals, namely 802.11b 1 Mbps, 802.11g 6 Mbps, and 802.11n MIMO-OFDM Single Stream (SS) 6.5 Mbps. In this scenario, we fix the positions of the Wi-Fi transmitter and the two tags, and move the receiver to increase the distance between the second-hop tag and the receiver (denoted by tag-to-RX distance). In addition, the Wi-Fi transmitter sends the excitation signal at Channel 2 with a central frequency of 2.417 GHz, and the Wi-Fi receiver listens on the backscattered signal at Channel 12 with a central frequency of 2.467 GHz. We collect the backscattered packet RSSI data and measure its changes at varying distances. The experimental results are reported as follows:

- *Rceived backscatter signal strength.* Figure 7.17 presents the results of the received backscatter signal strength (i.e., RSSI information). We can see that the received backscatter signal strength presents a downward trend as the tag-to-RX distance increases. Additionally, we can observe that the backscattered signal strength for 802.11g/n drops below −80 dBm at a distance of 3 m, and the backscattered signal strength for 802.11b falls below −85 dBm at a distance of 8 m.
- *Backscatter throughput*. Figure 7.18 presents the results of the backscatter throughput. Several observations are concluded as follows. (i) The backscatter throughput in the three subfigures has a general trend of decreasing as the tag-to-RX distance increases. (ii) The backscatter throughput for 802.11b is up to 200 bps at 0.5 m and drops to 50 bps when the distance is 6.5 m. (iii) The 802.11g/n backscattered signal achieves a communication distance of up to 3 m and a bit rate of up to 60 bps. In comparison with HitchHike [23], which is a single-hop backscatter scheme and can achieve a backscatter bit rate of up to 300 Kbps with a communication distance of up to 34 m, such backscatter throughput is very limited owing to the following two reasons. On the one hand, the attenuation of multi-hop paths restricts the tag-to-tag distance and weakens the signal strength of the last hop, thereby causing a limited throughput. To reduce decoding complexity, on the other hand, each tag is assigned a specific portion of PPDU data fields to embed its data, which limits the number of tag data embedded in a packet, thereby impacting the throughput.
- *Tag bit error rate (BER)*. Figure 7.19 presents the results of tag data BER. we can see that the BER values are less than 0.1 within a communication range of 0.5 m, which holds for 802.11b 1 Mbps, 802.11g 6 Mbps, and 802.11n SS 6.5 Mbps. In addition, we can observe that for the three different protocols, the BER values have a slight rise as the distance increases.

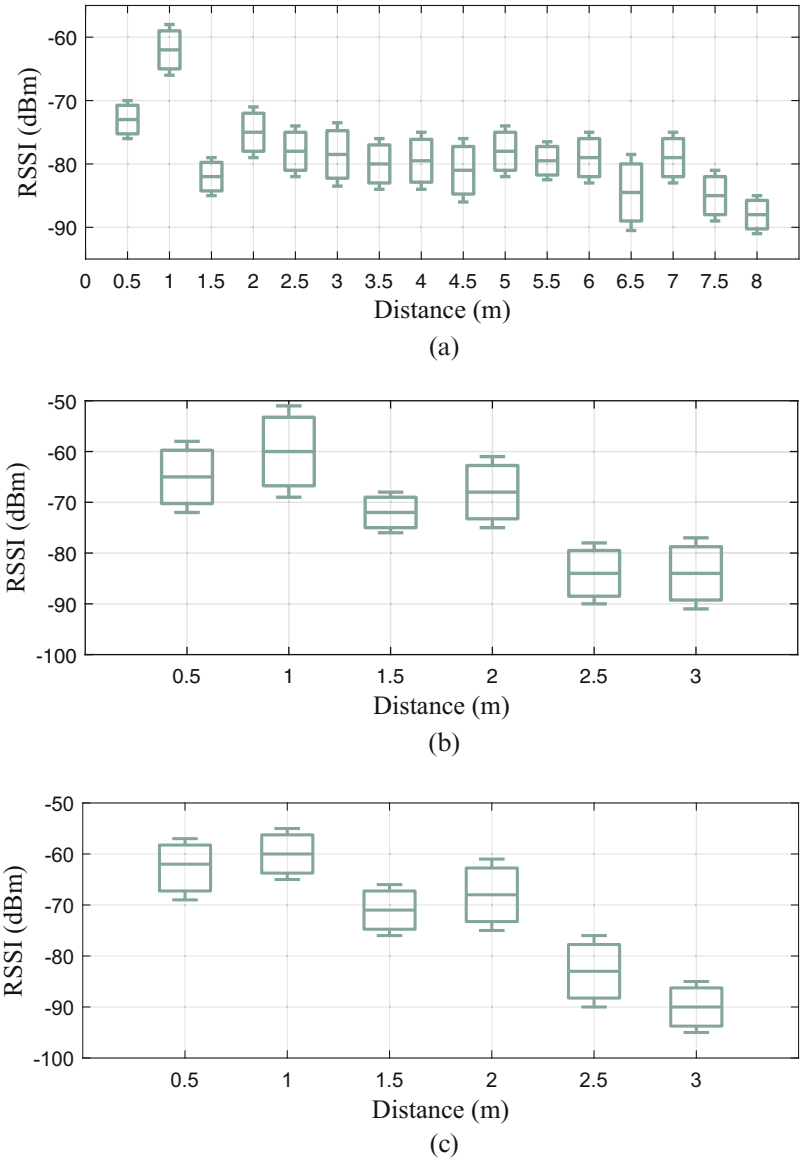


Fig. 7.17 The measured RSSI varying the distance between tags and Wi-Fi receiver. (**a**) 802.11b 1 Mbps. (**b**) 802.11g 6 Mbps. (**c**) 802.11n SS 6.5 Mbps

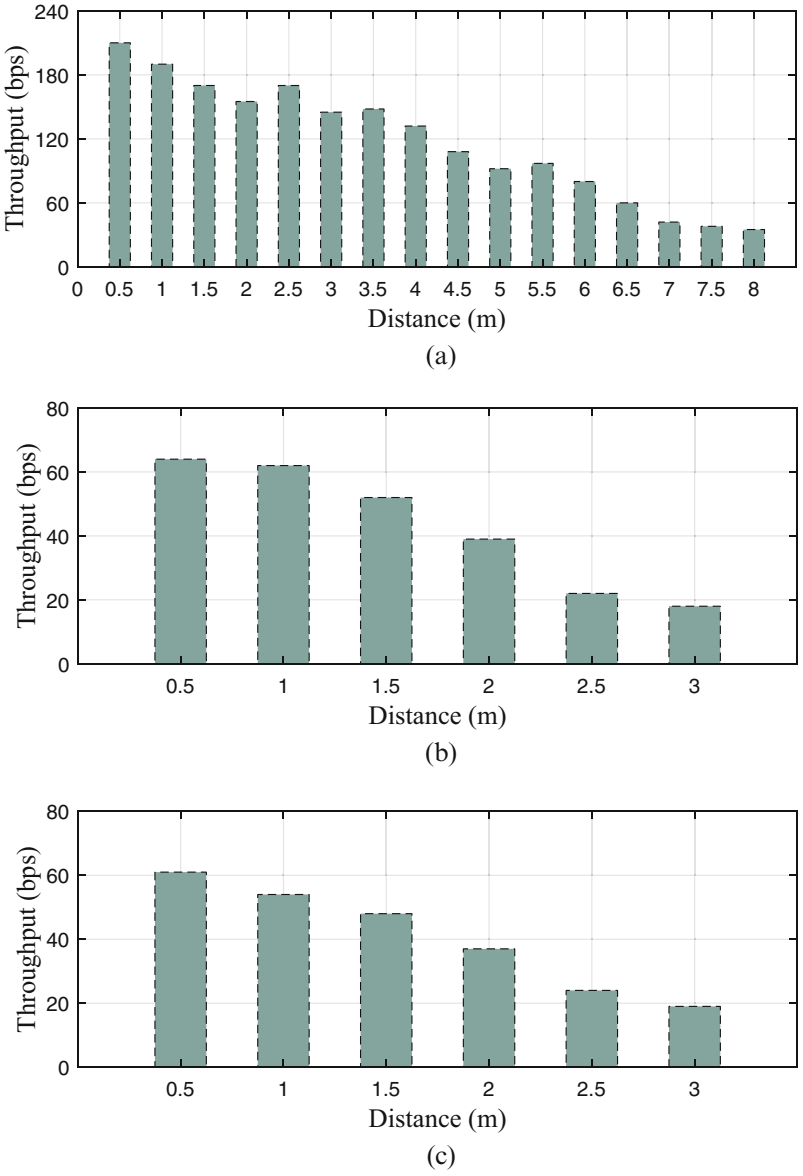


Fig. 7.18 The throughput varying the distance between tags and Wi-Fi receiver. (**a**) 802.11b 1 Mbps. (**b**) 802.11g 6 Mbps. (**c**) 802.11n SS 6.5 Mbps

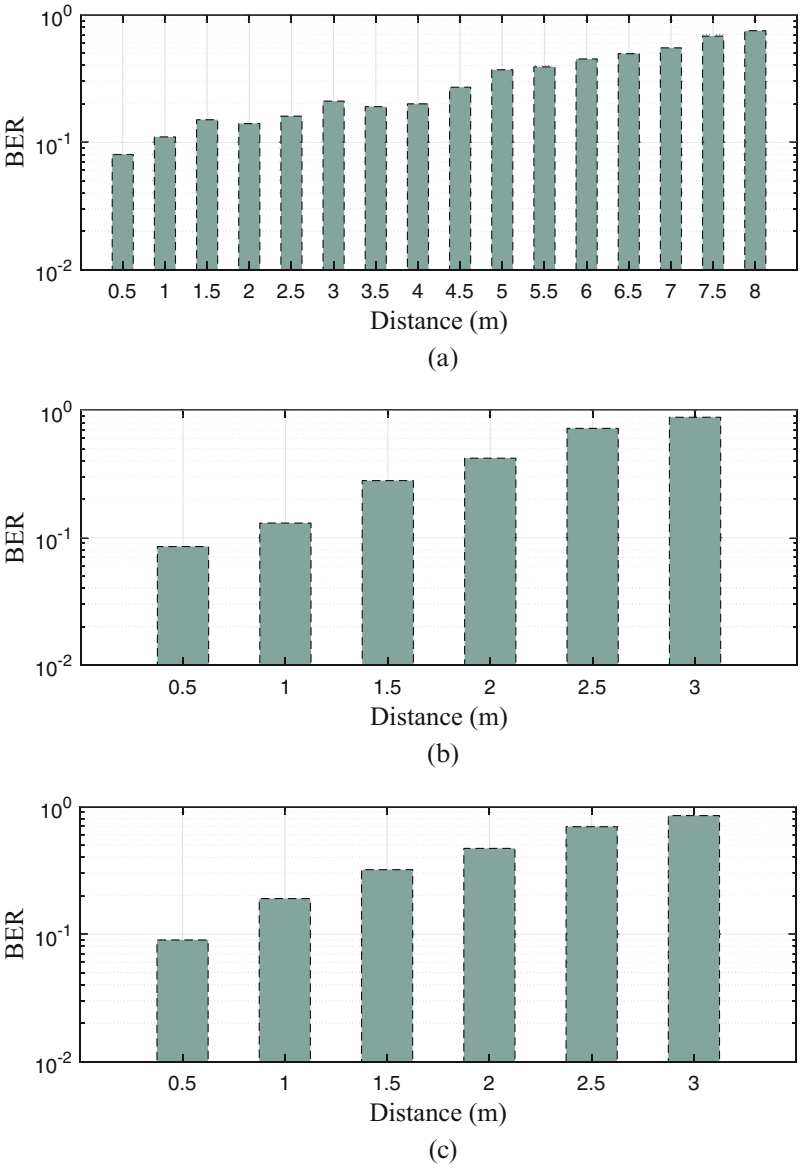


Fig. 7.19 The BER varies at different distances between tags and Wi-Fi receiver. (**a**) 802.11b 1 Mbps. (**b**) 802.11g 6 Mbps. (**c**) 802.11n SS 6.5 Mbps

Besides, we also evaluate our system in the non-line-of-sight scenario. Our measurements indicate a communication range of less than 0.5 m with a weak signal strength of less than −80 dBm.

7.5.2.2 Tag-to-Tag Distance

In terms of tag-to-tag distance, its performance is evaluated under the indoor scenario (see Fig. 7.15). In our implementation, (i) the positions of the transmitter, the first-hop tag, and the receiver are fixed; (ii) the receiver is placed two meters away from the first-hop tag; (iii) we move the second-hop tag to vary the tag-to-tag distance. The results are shown in Fig. 7.20. We can observe that the throughput and the BER have a degradation with the increment of the tag-to-tag distance. In addition, we can observe that when the distance between the two tags is 0.05 m, a bit rate of about 200 bps is obtained and the corresponding BER is about 0.08.

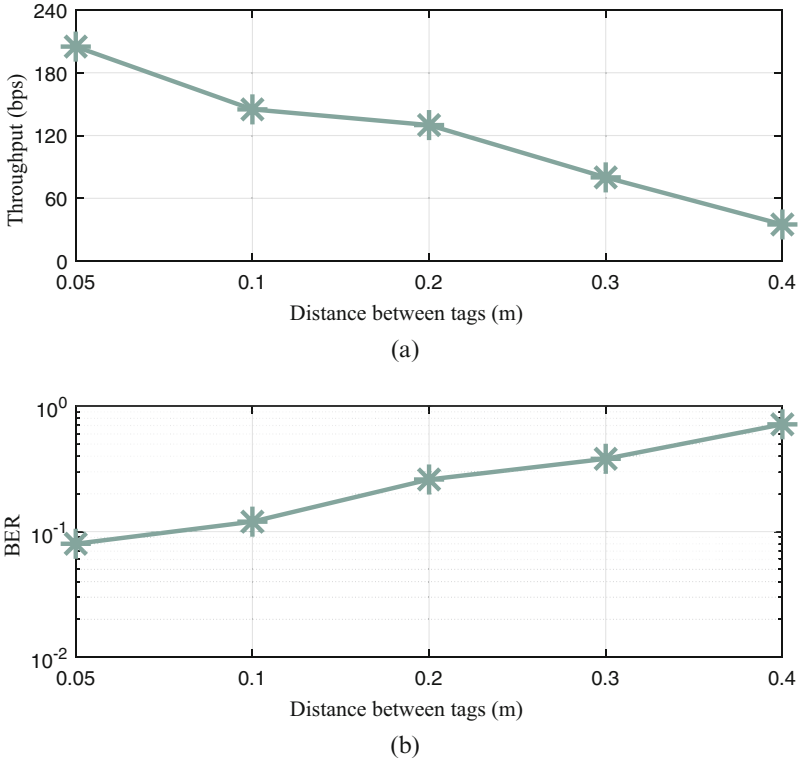


Fig. 7.20 Performance of multi-hop backscatter communication varying the distance between two tags. (**a**) Throughput. (**b**) Bit error rate

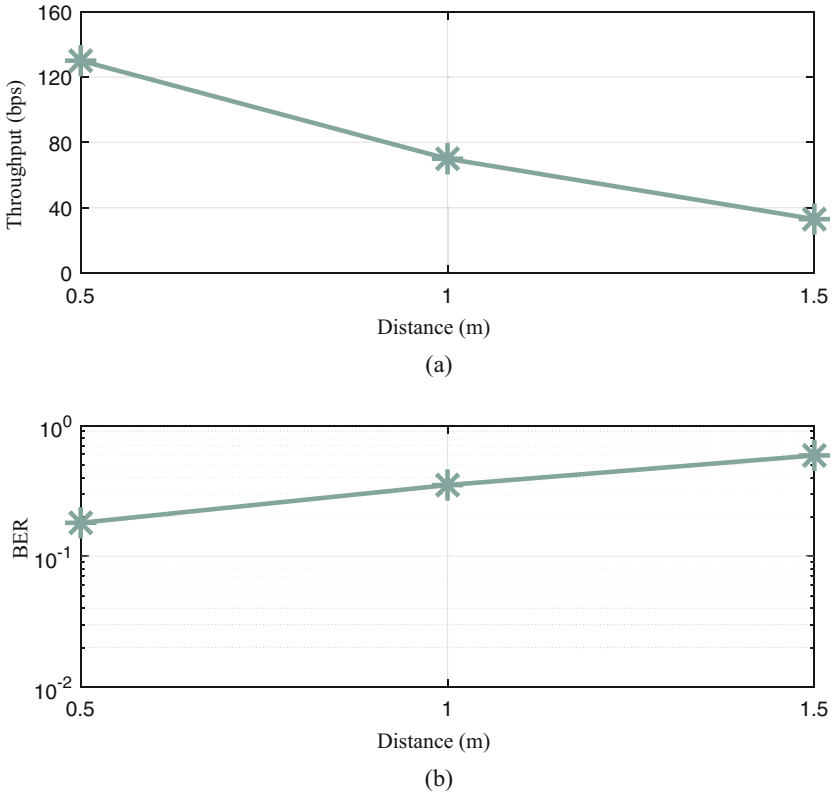


Fig. 7.21 Performance of adopting tag relay in the presence of obstacles. (**a**) Throughput. (**b**) Bit error rate

7.5.2.3 Obstacles

We use the scenario depicted in Fig. 7.16 to measure the effect of obstacles. In the case of the no-tag relay shown in Fig. 7.16a, our measurements reveal that more than 90% of packets experience signal levels below 85 dBm and bit rates below 10 bps with a communication range of less than 0.15 m. However, in the case of the tag relay depicted in Fig. 7.16b, our results depicted in Fig. 7.21 indicate a significant improvement. In particular, the throughput and the communication range are improved to 135 bps and up to 1.5 m, respectively.

7.5.2.4 Power Analysis

Our tag prototype utilizes the FPGA to implement various circuits, such as the control signal detection circuit and the phase modulation circuit. We evaluate their power consumption by using the XPower, which is a tool that has been

frequently used for measuring power consumption. Our measurements show that the overall power consumption is 14.2 mW, in which the DCM IP core for phase modulation consumes most of the power. Some power-efficient frequency shifting designs like the low-power phase-lock loop [21] and the ring oscillator [22] can be adopted to replace the energy-hungry DCM design. Other power-saving techniques include employing analog modulation circuits and low-power FPGAs[2] on the tag side. Further reductions in power consumption can be achieved using IC design approaches [21–24, 31–33].

7.6 Application Case

Multi-hop backscatter communication is expected to be widely used in various Internet-of-Things (IoT) applications, such as health care and autonomous vehicles. In this section, we briefly discuss these applications.

7.6.1 Health Care

Health care plays an extremely crucial role in ensuring the well-being of individuals. It can help to prevent disease and improve the quality of life of individuals. Multi-hop backscatter communication can be used to assist in the health care system. Such an example is shown in Fig. 7.22a, in which a man is running and sensing tags are attached to his on-body. These sensing tags can collect his physiological signs (e.g.,

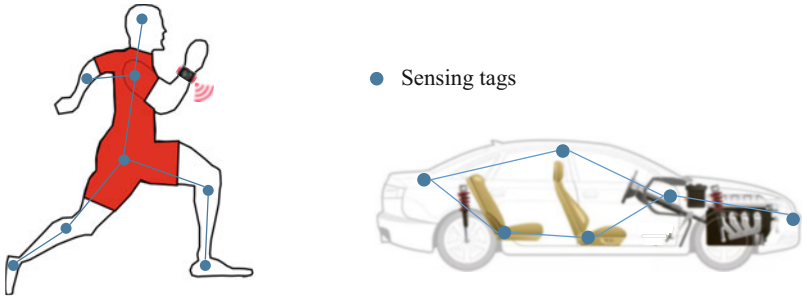


Fig. 7.22 Potential IoT applications empowered by multi-hop backscatter. (**a**) Health-care system. (**b**) Autonomous vehicle

[2] https://www.xilinx.com/products/technology/power.html, http://www.actel.com/FPGA/handheld/?p=sn.

heart rate and body temperature) and transmit those physiological signs to a receiver (e.g., a smartwatch) with the help of multi-hop backscatter communications. In this way, the runner can know his physical condition timely and take an action (e.g., speed up, slow down, or maintain his current pace), thereby reducing the risk of injury and maintaining good health.

7.6.2 Autonomous Vehicles

Multi-hop backscatter communication can also be used to assist autonomous vehicles. Specifically, backscatter tags can be flexibly deployed inside and on the surface of the vehicle. These tags can sense the environment around the vehicle by connecting sensing sensors and report the collected data to the in-car control center. Owing to the existence of obstacles (e.g., seat and car window), the channel between the tag and the receiver may be unreliable. As a result, the actual situation around the vehicle may not be truly reflected, thereby probably leading to an inappropriate action (e.g., sudden acceleration). This inappropriate action may endanger the safety of pedestrians. Multi-hop backscatter can leverage tag relay as an alternative path, which provides path diversity and robustness, as well as addresses unreliable channels, thereby enabling robust sensor data transmission As a result, the real situation can be obtained, thereby increasing the safety of autonomous driving. Such vision is depicted in Fig. 7.22b.

7.7 Summary and Discussion

In this chapter, we have presented a multi-hop backscatter system working with off-the-shelf Wi-Fi devices. We have first introduced the motivation for using multi-hop backscatter communication. Then, the Wi-Fi PHY primer has been briefly discussed. After that, we have presented a detailed discussion on the system design. Next, we have provided the implemental details and reported numerous experimental results. The experimental results have verified the feasibility and effectiveness of our system, especially when tags encounter physical obstacles. Finally, we have discussed several potential applications driven by multi-hop backscatter communication. Our system enables tags to transmit their data in sequence, which differs from concurrent transmission where multiple tags transmit data at the same time. However, concurrent transmission schemes can be used to extend our system, such as enabling multiple groups of tag-relay communications. But such an implementation is beyond the scope of this work. In summary, we believe that our multi-hop backscatter system takes a crucial step toward ubiquitous communication. Although our multi-hop backscatter system has shown its various advantages, it still faces a series of challenges, which we discuss as follows:

1. ***Analog forwarding vs. digital forwarding***. There are two potential approaches, (i) analog forwarding and (ii) digital forwarding, that can be used to enable multi-hop backscatter communication. In comparison with digital forwarding where a tag needs to decode the incoming signal after forwarding these signals, analog forwarding simply forwards the incoming signals without decoding, thereby reducing hardware complexity for the tag. In addition, decoding the backscattered signals generally requires power-hungry components, which are infeasible for low-power tags. Therefore, our tag uses analog forwarding. However, a key issue is the signal attenuation in analog forwarding, since the power of the RF signal will become significantly weak after undergoing several reflections. As a result, the backscattered signal may be too weak to use for decoding when the number of reflections surpasses two, thereby causing a limited communication range. One potential solution to address this limitation is leveraging long-range communication techniques, such as LoRa [34, 35]. The implementation of such a solution is left for future work.
2. ***Dynamic frequency shift and receive channel setting***. While our tag can operate in the following two modes: (i) the relay mode and (ii) the non-relay mode, the frequency shift setting in each tag is constant at 25 MHz and the receive channel is also fixed at channel 12. As a result, the performance of the system may be degraded when communication channels are unreliable, or there are collisions among multiple tag-relay groups owing to the absence of MAC mechanisms. Potential solutions include the design of a dynamic frequency shift scheme and an adaptive receive channel setting.
3. ***Limited throughput***. Although the experimental results demonstrate that our multi-hop backscatter system provides path diversity and robustness, and achieves a throughput of up to 200 bps for the two-hop case, such throughput is very restricted in comparison with a single-hop backscatter scheme (e.g., HitchHike [23]), as discussed in Sect. 7.5.2.1. One possible solution is leveraging the entire data fields of a packet for modulation rather than a portion of the data fields. The implementation of such a solution is left for future work.

References

1. Yuan L, Gong W (2022) Subscatter: sub-symbol wifi backscatter for high throughput. In: 2022 IEEE 30th international conference on network protocols (ICNP). IEEE, Piscataway, pp 1–11
2. Xu Z, Gong W (2022) Enabling zigbee backscatter communication in a crowded spectrum. In: 2022 IEEE 30th international conference on network protocols (ICNP). IEEE, Piscataway, pp 1–11
3. Yang Y, Yuan L, Zhao J, Gong W (2022) Content-agnostic backscatter from thin air. In: Proceedings of the 20th annual international conference on mobile systems, applications and services, pp 343–356
4. Huang Z, Gong W (2022) Eascatter: excitor-aware bluetooth backscatter. In: 2022 IEEE/ACM 30th international symposium on quality of service (IWQoS). IEEE, Piscataway, pp 1–10

5. Yang Y, Gong W (2022) Universal space-time stream backscatter with ambient wifi. In: 2022 IEEE international conference on pervasive computing and communications (PerCom). IEEE, Piscataway, pp 101–110
6. Wu, W, Wang, X, Hawbani A, Yuan L, Gong W (2022) A survey on ambient backscatter communications: principles, systems, applications, and challenges. Comput Netw 216:109235
7. Yuan L, Xiong C, Chen S, Gong W (2021) Embracing self-powered wireless wearables for smart healthcare. In: 2021 IEEE international conference on pervasive computing and communications (PerCom). IEEE, Piscataway, pp 1–7
8. Gong W, Yuan L, Wang Q, Zhao J (2020) Multiprotocol backscatter for personal IoT sensors. In: Proceedings of the 16th international conference on emerging networking experiments and technologies, pp 261–273
9. Yuan L, Zhang R, Yang K, An J, Chen S, Gong W (2020) Protocol-aware backscatter communication using commodity radios. In: 2020 IEEE/CIC international conference on communications in China (ICCC). IEEE, Piscataway, pp 336–341
10. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of the 16th annual international conference on mobile systems, applications, and services, pp 191–203
11. Jiang M, Gong W (2023) Bidirectional bluetooth backscatter with edges. IEEE Trans Mobile Comput, early access. https://doi.org/10.1109/TMC.2023.3241202
12. Feng Y, Gong W (2022) LTE-like paging and synchronization for ambient backscatter. In: GLOBECOM 2022-2022 IEEE global communications conference. IEEE, Piscataway, pp 2038–2043
13. Jiang M, Feng Y, Nayak A, Gong W (2022) Enabling high-goodput backscatter communication with commodity BLE. In: ICC 2022-IEEE international conference on communications. IEEE, Piscataway, pp 2242–2247
14. Raiciu C, Barre S, Pluntke C, Greenhalgh A, Wischik D, Handley M (2011) Improving datacenter performance and robustness with multipath TCP. ACM SIGCOMM Comput Commun Rev 41(4):266–277
15. Zhao J, Liu J, Wang H, Xu C (2017) Multipath TCP for datacenters: from energy efficiency perspective. In: IEEE INFOCOM 2017-IEEE conference on computer communications. IEEE, Piscataway, pp 1–9
16. Gnawali O, Fonseca R, Jamieson K, Moss D, Levis P (2009) Collection tree protocol. In: Proceedings of the 7th ACM conference on embedded networked sensor systems, pp 1–14
17. Wu W, Wang X, Hawbani A, Liu P, Zhao L, Al-Dubai A (2021) Flora: fuzzy based load-balanced opportunistic routing for asynchronous duty-cycled WSNS. IEEE Trans Mobile Comput 22(1):253–268
18. Kellogg B, Parks A, Gollakota S, Smith JR, Wetherall D (2014) Wi-fi backscatter: internet connectivity for RF-powered devices. In: Proceedings of the 2014 ACM conference on SIGCOMM, pp 607–618
19. Bharadia D, Joshi KR, Kotaru M, Katti S (2015) Backfi: high throughput wifi backscatter. ACM SIGCOMM Comput Commun Rev 45(4):283–296
20. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In: 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16), pp 151–164
21. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 356–369
22. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 370–383
23. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: practical backscatter using commodity wifi. In: Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM, pp 259–271

24. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In: Proceedings of the 13th international conference on emerging networking experiments and technologies, pp 389–401
25. Ma Y, Selby N, Adib F (2017) Drone relays for battery-free networks. In: Proceedings of the conference of the ACM special interest group on data communication, pp 335–347
26. Zhao J, Gong W, Liu J (2018) X-tandem: towards multi-hop backscatter communication with commodity wifi. In: Proceedings of the 24th annual international conference on mobile computing and networking, pp 497–511
27. IEEE STD 802.11-1999. Wireless lan medium access control (MAC) and physical layer (phy) specifications
28. IEEE STD 802.11a-1999. Wireless lan medium access control (MAC) and physical layer (phy) specifications: high-speed physical layer in the 5 ghz band
29. IEEE STD 802.11g-2003. Wireless lan medium access control (MAC) and physical layer (phy) specifications, amendment 4: further higher data rate extension in the 2.4 ghz band
30. IEEE STD 802.11n-2009. Wireless LAN medium access control (MAC) and physical layer (phy) specifications, amendment 5: enhancements for higher throughput
31. Wang A, Iyer V, Talla V, Smith JR, Gollakota S (2017) FM backscatter: enabling connected cities and smart fabrics. In: 14th USENIX symposium on networked systems design and implementation NSDI, vol 17, pp 3154630–3154650
32. Talla V, Hessar M, Kellogg B, Najafi A, Smith JR, Gollakota S (2017) Lora backscatter: enabling the vision of ubiquitous connectivity. Proc ACM Interactive Mobile, Wearable Ubiq Technol 1(3):1–24.
33. Naderiparizi S, Hessar M, Talla V, Gollakota S, Smith JR (2018) Towards battery-free {HD} video streaming. In: 15th {USENIX} symposium on networked systems design and implementation ({NSDI} 18), pp 233–247
34. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) Plora: a passive long-range data network from ambient lora transmissions. In: Proceedings of the 2018 conference of the ACM special interest group on data communication, pp 147–160
35. Vasisht D, Zhang G, Abari O, Lu HM, Flanz J, Katabi D (2018) In-body backscatter communication and localization. In: Proceedings of the 2018 conference of the ACM special interest group on data communication, pp 132–146

Chapter 8
Multi-Hop Backscatter Sensor Mesh

Abstract Existing backscatter schemes typically rely on a single source and can only communicate within one hop. Many studies show that multi-hop backscatter communication is feasible. However, in existing work, the transmission of multi-hop signals is subject to severe fading, which limits the quality and range of communication. This chapter presents a decoded tag relay solution designed to enable scalable deployments using distributed excitation to build an innovative wireless sensor mesh. The mesh enables simultaneous sensing and relaying, overcoming the limitations of multi-hop signal fading in existing schemes and significantly improving data throughput and communication range.

8.1 Introduction

When creating a large multi-hop sensor mesh, the following problems usually arise. The first is the problem of energy limitation [1]. In networks, sensor nodes need to collect and transmit various data to perform their required tasks. These operations usually consume more energy, while the general sensor nodes need battery power. And the battery capacity is limited. The imbalance of energy consumption will lead to node energy depletion or even failure. And large-scale networks have many sensor nodes. The energy supply is huge and complex. Therefore, how to optimize the energy supply of sensor nodes and extend the service time is an issue. Secondly, the maintenance of network reliability is also an important problem to be solved. For example, in a sensor network that monitors the production of a large factory, as the size of the factory expands, more sensor nodes must be added continuously to cover a larger area and monitor more parameters [2]. However, with the increase of nodes' number, the communication load and data processing load of the network will also increase, which may lead to a decrease in the performance and reliability of the network.

Researchers have made many efforts to build new sensor networks [3–7]. Low-power backscatter sensing devices provide a better solution [8–12]. The backscatter tags can collect energy from ambient signals (such as Wi-Fi, Bluetooth, visible light and sound, etc.) to support communication, and transmit sensing

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_8

data using environmental signals as carriers. Therefore, the devices don't need frequent battery replacement, and they can also save transmission power. It improves the energy efficiency and reliability of the sensor network, and facilitates large-scale deployment. In existing works, the backscatter-based sensor network has wide applications in temperature detection [11], motion monitoring [12], and sound monitoring [13], such as warehouse temperature control system, security system, smart home, etc. Most of these designs use single-hop mode yet. So The communication distance is limited. It obstacles the deployment of sensor networks and cannot be applied to application scenarios that require large-scale monitoring. And the single-hop backscatter sensor network can only rely on a single excitation source for communication. So it is difficult to support high-speed transmission of much data.

If the tag has the function of the relay, the backscatter sensor mesh can improve the transmission quality and change from single-hop mode to multi-hop mode. In the multi-hop backscatter system, the source node first transmits the RF signal, which is transmitted to the nearest relay node. After receiving the signal from the source node, the relay node will perform a backscattered operation and forward the signal to other nodes around it. The nodes can relay to each other. When the sensor node is close to the reader, the sensor data can also be returned directly to the reader to form a two-way communication. X-Tandem, for example, is an operating model for a multi-hop backscatter system using commodity Wi-Fi. Its sensor tags can be interconnected as relay stations. The experimental data show that the backscatter throughput of the X-Tandem with double hops can be increased by more than 10 times compared with the single-hop solution in an indoor environment with obstacles. However, when we implement the three-hop backscatter system with 802.11n Wi-Fi excitation in the same way, we find that the signal attenuation is serious with the increasing number of hops, especially when the third hop is performed, the noise intensity is even higher than the backscatter signal, and the signal can't be transmitted. As shown in Fig. 8.1, the reason for multi-hop signal attenuation can be attributed to the fact that X-Tandem [14] is a backscatter

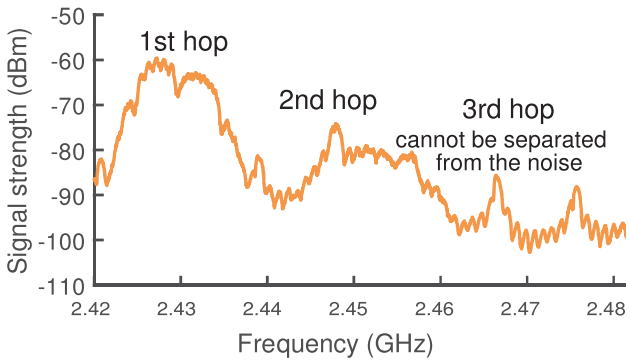


Fig. 8.1 Severe attenuation when using centrally excited and non-decodable tag relays

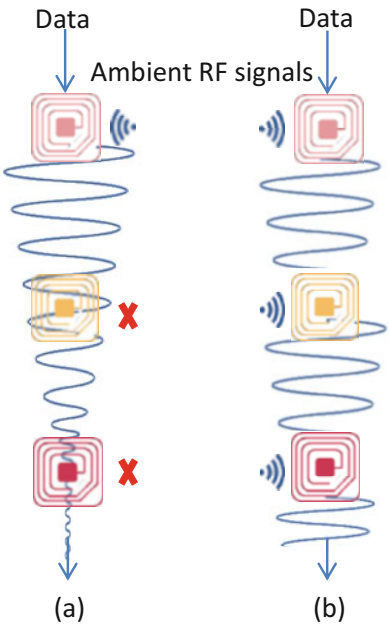


Fig. 8.2 Different ways in multi-hop backscatter: (**a**) non-decodable relay tags only use first-hop ambient signals; (**b**) ambient signals for each tag improve the strength of multi-hop signal

system with centralized excitation and its relay tags are not decodable. Firstly, the centralized excitation must be provided by the central node with limited coverage. It increases the cost and mobility of the network if multiple central nodes are used to provide the excitation signals. The left half of Fig. 8.2 shows that the non-decodable nature allows tags to only backscatter the first hop signal directly. The backscatter signals received by tags further away from the excitation have been reflected several times and therefore the signal is severely attenuated.

To reduce the cost and complexity of the network, we hope to use distributed rather than centralized excitation. In our life, mobile phones, computers, routers and other devices already exist on a large scale. We can use them as natural distributed excitation sources to improve communication quality at no additional cost. It's shown in the right half of the Fig. 8.2. And as shown in Fig. 8.3, the decoded relay and distributed excitation can greatly expand the coverage of the sensor network and bring low power consumption, high throughput, standby path, robustness compared with the centralized mode. We also expect that the signal attenuation can be reduced by enabling the decoding tag relay while using distributed excitation. However, there are a number of challenges. (1) The sensor data is represented by the baseband signal before the jump. We need to redesign the baseband circuit to reduce the decoding workload. (2) The signal is gradually attenuated in the backscatter process, which will affect envelope detection. (3) We also need to ensure the real-time of sensing data while maintaining the relay capability of the tag. This means that the relay request and detection data tasks between tags must be implemented in parallel.

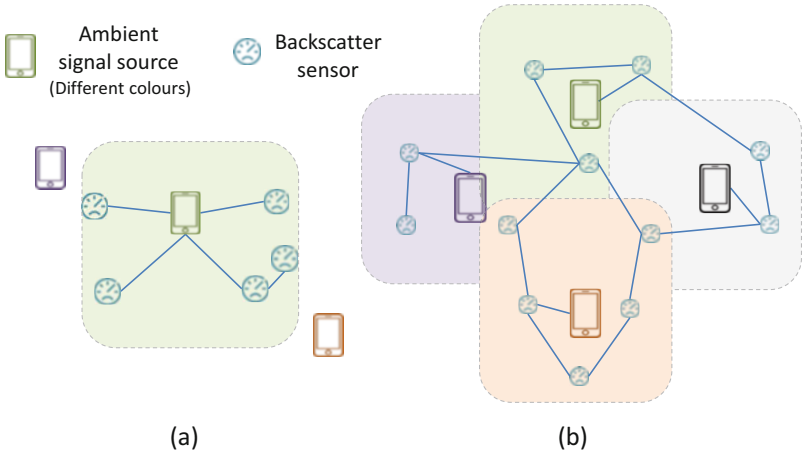


Fig. 8.3 Comparison of two types of backscatter sensor networks: (**a**) use centralized excitation and non-decodable relay; (**b**) use distributed excitation and decodable relay

In this chapter, we introduced a new multi-hop backscatter sensor mesh, DecRel. It uses the distributed excitation mode to enable the decoded tag relay, which is an innovative wireless sensor architecture that can simultaneously sense and relay.

8.2 Related Work

Backscatter-Based Sensors RFID (Radio Frequency Identification) is a traditional backscatter system that is widely used [15–22]. People usually embed temperature or shock detection sensors into labels according to their needs. For example, the RFID system with temperature sensor is used to detect the granary environment, and the RFID system with shock detection sensor is combined with the logistics management system to reduce unnecessary losses during transportation. However, the RFID system has some limitations. It requires a special reader to send a specific frequency of RF signal to the passive tag, and to ensure measurement accuracy, the reader must be deployed every ten meters in a specific detection environment. In addition to the daily maintenance, the cost is high [23]. Ambient backscatter technology has attracted more attention. It can convert existing wireless signals into power sources and communication media. At present, environmental backscatter technology has explored various RF signals available in the environment (for example, TV, cellular, Wi-Fi, etc.) [1]. For example, the design of smart contact lenses [24] equipped with blood glucose sensors can use Bluetooth and Wi-Fi signals to send patients' blood glucose information in real time with backscatter communication. In addition to the transmission of scalar data, multimedia data can also be transmitted. For example, video Stream Backscatter [25] can use analogue backscatter technology to achieve

high-definition video stream transmission through a battery-free wireless camera. Our work is to implement a scalable and reliable multi-hop sensor network based on these works. It can not only realize the acquisition and synchronous transmission of sensor data, but also realize the decoding relay in the transmission process. The technology will make great contributions to the large-scale deployment of multi-hop sensor networks.

Multi-Tag Backscatter Networks Multi-tag backscatter networks also contribute to the development of backscatter systems. For example, traditional RFID systems usually include readers, antennas, and many tags. Multiple tags can backscatter signals to achieve communication and data transmission with the reader-writer. In the existing work, there are also multi-tag backscatter systems that can be stimulated by Bluetooth and ZigBee, such as FreeRider [26]. It can allocate time slots for the simultaneous transmission of multiple tags by using MAC protocol. Freerider, based on Bluetooth and ZigBee backscatter tags, can communicate with smartphones and achieve a wide range of tracking functions. To further expand the scale, we can introduce tag relay into the multi-tag backscatter network to improve the data transmission capability.

Mesh Networks With the explosive growth of Internet users, society needs to provide the Internet dynamically and efficiently on a large scale. To enable enterprise networks to have a low initial cost, easy network maintenance, and reliable service coverage, a wireless mesh network provides a new practical wireless solution [27]. It is a multi-hop-based topology that can provide community broadband Internet access services through efficient and dynamic organization and configuration of nodes in the network. The network mainly consists of four elements [28]. The Mesh Client (MC) is a wireless client, such as computers, smartphones, and other wireless devices. The Mesh Router (MR) is used to transfer data to and from the Gateway. The access point AP provides Internet access to MC by managing the aggregated traffic to MR. Finally, the Mesh Gateway (MG) plays a role in establishing the appropriate connection between the wireless infrastructure and the Internet. The advantage of mesh is that the mesh topology allows nodes to interconnect and self-organize to form a dynamic network. Wireless Mesh Networks (WMN) nodes can be added or removed at any time with a degree of scalability and robustness. The nodes in the mesh network can communicate over multiple links, improving the reliability and fault tolerance of the network. However, the nodes in the mesh network require multiple forwarding to complete communication. When the network size is large, the routing complexity and communication delay of the Mesh network will increase, resulting in a decrease in network performance [29]. We can refer to the topology of the Mesh network and implement the backscatter technology between nodes for communication. The communication between auxiliary nodes only needs a backscatter, which can meet the application requirements of low power consumption while achieving high performance.

8.3 Multi-Hop Backscatter Communication Background

Multi-hop backscatter communication systems typically consist of a source node, a relay node with a backscatter tag, and a receiver. The source nodes first transmit RF signals to excite the tags of the relay node for backscatter communication. In the process, when a node is required to send information to another node, it will encode the information into backscatter signals by modulating baseband signals and transmitting them. If the destination node is within the direct range of the transmitting node, the backscatter signal can be received directly by the destination node. Otherwise, the backscattered signal is forwarded by the relay tag node until it reaches the destination node. The relay tag nodes in multi-hop backscatter sensor networks play an important role. They can effectively expand the network coverage and the number of connected nodes, and improve the scalability of the network. The existence of relay tags can improve the efficiency of data transmission, and reduce the data transmission delay and energy consumption.

The existing research work mainly focuses on the protocol design, performance analysis, and system implementation of multi-hop wireless communication systems. For example, some researchers have proposed a new multi-hop wireless communication protocol to improve the efficiency of the system. Other researchers have studied the power management and optimization methods of multi-hop wireless communication system to improve the energy efficiency of the system. In addition, some researchers combine multi-hop wireless communication technology with other wireless communication technologies [30]. The technology plays an important role in the Internet of Things, and is usually used to build large-scale sensor networks. For example, intelligent transportation system can use Multi-hop backscatter communication technology to realize communication between vehicles, thus improving road safety and traffic efficiency. Multi-hop backscatter communication technology can realize long-distance communication between nodes in the traffic scene, thus developing the accuracy of intelligent transportation system.

However, in the construction of multi-hop backscatter sensor networks, attention should also be paid to the synchronous sensing characteristics of the system. Specifically, when multiple backscatter tags are activated to communicate with each other, time synchronization technology should also be used to ensure real-time sensing data.

8.4 Design

8.4.1 Overview

In this article, we mainly introduce the main components and working methods of the DecRel. As shown in Fig. 8.4, we focus on the design of the sensing path and the relay path. The sensing path is used to generate appropriate baseband signals,

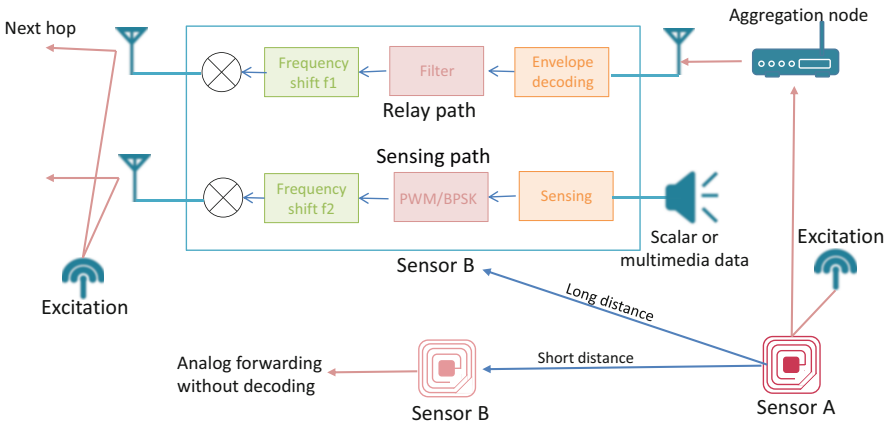


Fig. 8.4 Simutaneous sensing and relay in multi-hop backscatter sensor mesh

including digital baseband signals and analogue baseband signals. The relay path is used to help the tag decode the baseband signal of the previous hop. In order for the two paths not to interfere with each other, we use two frequency-shifted clock signals to solve this problem. Considering the mobility of tags, two relay modes are provided according to the distance in the design. At the same time, we provide reconfigurable tag operations according to the actual situation.

8.4.2 Sensing Path

8.4.2.1 Sensing Frontend

The data flow rate will change depending on the sensor transmitting different data. For example, when detecting temperature, the sensor can transmit data at the rate of tens of thousands of bits per second. When transmitting HD video streams, the transmission speed is in the tens to hundreds of megabits per second. Therefore, we have designed appropriate sensor front ends.

The digital sensing front-end consists of an external sensor and a readout device as shown in Fig. 8.5a. The readout device can be driven by ADC or hardware description language. External sensors can be added to the label as needed. The digital sensing front-end is suitable for measuring scalar data.

Compared with the digital sensor front-end, the analogue sensor front-end is more suitable for the collection of multimedia data, mainly for the following reasons. Firstly, it usually requires less energy consumption to simulate the multimedia data collected by the sensor front-end. For example, previous works [12, 25, 31] use low-power circuit design and deep-sleep technology to further reduce power consumption and improve endurance. Secondly, analogue sensor

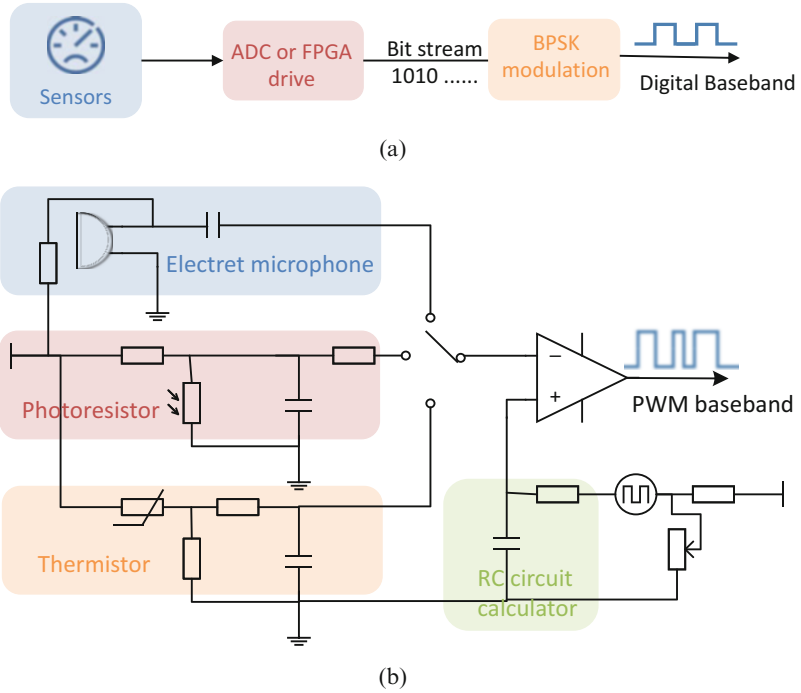


Fig. 8.5 Two types of sensing frontend and baseband modulation. (**a**) Digital sensing and baseband using BPSK. (**b**) Analog sensing and PWM baseband

front-end usually uses compression algorithms based on signal characteristics, such as wavelet transform and hadamard transform, which can achieve data compression under the assumption of ensuring data quality. At the same time, existing works show that small video streaming servers can be connected to client applications to separate transmission and computation [8]. In this way, a group of power-consuming components for computation, such as ADC, microprocessor, etc., can be removed to achieve lightweight transmission. The front end of the analogue sensor we designed uses a microphone, a photoresistor, and a thermistor to correspond to three types of analogue data: sound, light, and temperature. It's shown in Fig. 8.5b.

8.4.2.2 Baseband Modulation

After collecting the sensing signals, the tag needs to modulate them into a baseband signals for transmission. Since we use both digital and analogue sensing front-ends, we need to modulate digital baseband and analogue baseband respectively.

The bits converted by the digital sensing front-end flow through the digital baseband circuit and are converted into a continuous voltage level of fixed length,

where 1 indicates high level and 0 indicates low level. Then BPSK is used to modulate the digital baseband into binary amplitude as shown in Fig. 8.5a.

For analogue measurement data, we use a pulse width modulation circuit to generate analogue baseband as shown in Fig. 8.5b. The pulse width modulation circuit can convert the analogue signal into the corresponding pulse signal, and modulate the analogue signal by controlling the width of the pulse signal. The main part of the circuit includes a comparator, a timer, and an RC circuit calculator. The comparator compares the input analogue signal with the periodic triangular wave generated by the RC circuit to produce a periodic PWM baseband signal. The timer measures the duration of the pulse signal and converts it to a digital signal for subsequent digital signal processing.

8.4.3 Relay Path

8.4.3.1 Envelope Detection

In tag relay, each tag receives the frequency hopping signals from the other tags and converts them into baseband signals for processing and forwarding. This will help the tag not to have to recover the original data. The key is to get the correct baseband signal. Since the frequency of the high frequency signal is constantly changing, the relay tags must use envelope detection technology to detect the envelope of the high frequency signal. By using envelope detection, the relay tags can extract the baseband signal of the frequency hopping signal. Then they use amplitude demodulation technology to obtain the amplitude information of the baseband signal. So we need an envelope detector. The envelope detector filters out the high frequency components of the signal by rectifying, low-pass filtering and amplifying the signal. They leave only the baseband components to extract the signal envelope. An envelope detector usually consists of a double diode rectifier, an antenna and other components. As shown in Fig. 8.6, the double diode rectifier is used to convert the AC signal into a DC signal. It consists of two diodes in reverse parallel, which can significantly improve the detection sensitivity and range. We record the output of envelope detector. Figure 8.7a shows the digital baseband envelope of the detected '1' repeated transmission. Figure 8.7b shows the detected analogue baseband envelope, which is part of the analogue signal sampled and modulated with a 48 kHz pulse width.

8.4.3.2 Correlation Between Sensing Path and Relay Path

In multi-hop backscatter sensor networks, the relay path of the tag has some correlation with the sensing path of the previous-hop tag. There are three advantages for the tag to relay by amplitude demodulation of the baseband signal. Firstly, the decoding scheme is simplified and the consumption is reduced. We can extract the

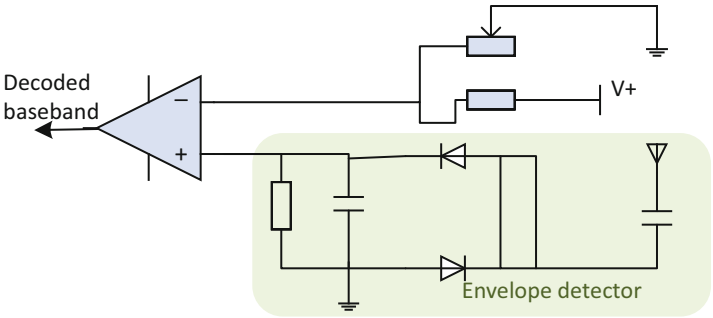


Fig. 8.6 Envelope detector circuit

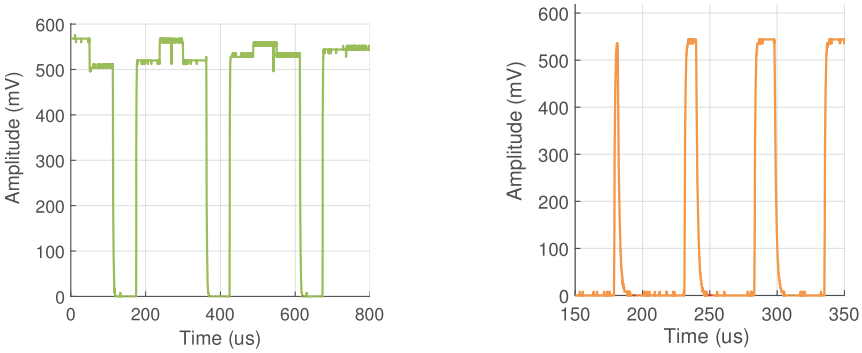


Fig. 8.7 The output trace of envelope detector. (**a**) Digital baseband signal with BPSK. (**b**) Analog baseband signal with PWM

baseband signal and demodulate its amplitude with a simple envelope detector. The envelope detector in our design consumes less power because the high-frequency oscillator and external power supply have been removed. Secondly, by eliminating some baseband circuitry, the relay path circuit is more portable than the sensor path circuit. Thirdly, in amplitude modulation, the information is modulated to the amplitude of the carrier signal. Therefore, amplitude demodulation can separate the information of the modulated signal from the carrier signal and make it a separate baseband signal. This baseband signal can be processed directly in the analog baseband circuit without complicated high-frequency signal processing. It can greatly simplify the circuit and reduce the cost.

8.4.3.3 Aggregation Node

The nodes in a multi-hop backscatter network need to communicate by receiving and reflecting radio signals. In such a mesh, nodes that are far away from each other

need multiple hops to communicate, so a large number of signal losses and energy consumption will be generated. The aggregation node can receive and aggregate signals from multiple tags and forward them to the next level relay node or the node of the base station. When relaying, the aggregation node not only forwards signals, but also assists in tag decoding. Especially when the distance between two tags is very large, the backscatter signal level of the forward hop is often too weak to be detected by the envelope detector of the backward hop. The aggregation node can demodulate the baseband signal first, and then broadcast it. Aggregated nodes can provide signals with better amplitude and clarity, and improve the accuracy of tag decoding.

8.4.4 Simultaneous Backscatter for Two Paths

When the backscatter tags receive the sensing data, they will use modulation technology to modulate the data into their own backscatter signals, and then adjust the impedance of the antenna for backscatter communication. The sensing path and relay path in this design need to participate in the backscatter communication process. However, we need to solve a problem. When the relay tag receives the backscattered signal, it will also receive the excitation signal. They can share the same frequency band, and the excitation signal is 30 dB higher than the backscatter signal. Referring to previous works, such as HichHike [32], frequency shifting is used to eliminate the interference between the sensing and relay paths. In this design, we assign two different frequency bands to the excitation signals of the two paths to solve this problem. Figure 8.8 shows the experimental results of synchronous sensing and relay. Figure 8.8a shows that the first hop tag uses the 10 MHz frequency offset of the excitation signal to backscatter the data to the center

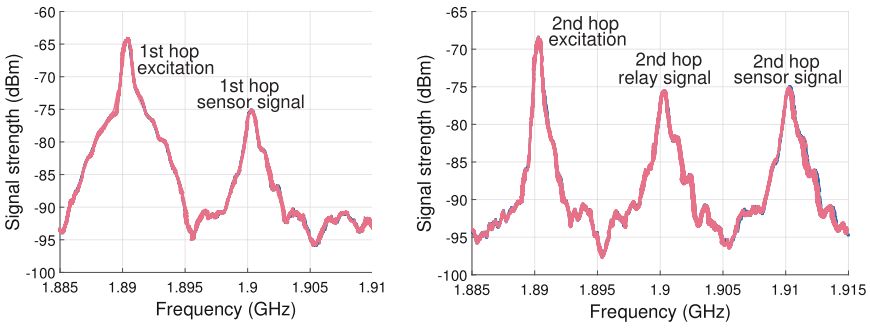


Fig. 8.8 Two hop tags frequency spectrum. (**a**) The first hop tag's frequency spectrum. (**b**) The second hop tag's frequency spectrum

frequency. As shown in Fig. 8.8b, the relay path of the second hop tag uses a 10 MHz frequency offset and the sensing path uses a 20 MHz frequency offset.

8.4.5 Reader Demodulation

When the backscatter tag returns data to the reader, the data information can be modulated to the single-tone carrier for transmission. The reader multiplies the received signal with a reference signal of known frequency to remove the tone carrier in the signal and extract the modulation information. Finally, as shown in Fig. 8.8b, we can obtain a 10 MHz relay signal and a 20 MHz sensor signal. In backscatter communication, the tag uses a modulation circuit to modulate the baseband signal on the backscatter signal. Among them, tags usually use high-frequency square-wave signals to perform XOR operation on baseband signals to generate modulated signals. The 10 MHz or 20 MHz signal is modulated on the baseband binary amplitude value, and the baseband amplitude value is modulated with a 180° phase offset. Therefore, using quadrature phase discrimination, baseband signals can be extracted from phase modulated 10 MHz or 20 MHz signals. Figure 8.11 shows the trace of the demodulated backscattered signal of time-varying pulse width analog data.

8.4.6 Relay Mode and Reconfiguration of Tags

In real-world deployments, the distance between tags is variable, so the system provides an alternative method of relaying tags: if the distance between two tags is long, the second-hop tag can use its decoding capabilities to maintain a high-quality relay connection. If the distance between the tags is short, the second hop tag can be reconfigured for analog transmission, which can be achieved by performing frequency conversion at very low power. The tag can also be reconfigured by other operations such as enabling or disabling digital or analog baseband circuitry, or selecting a different clock signal for the frequency offset.

8.5 Performance Evaluation

8.5.1 Implementation

In this section, analog and digital FPFA circuits are used to realize basic functions and a PCB prototype of the backscatter tag is built, as shown in Fig. 8.9. We also carry out power analysis and optimization of IC designs.

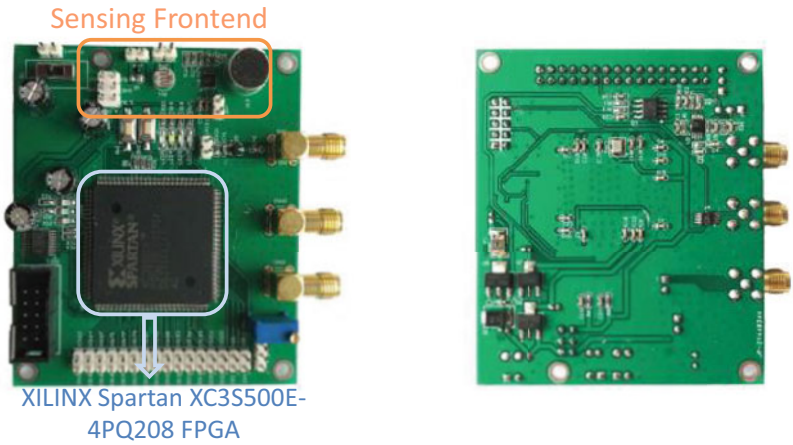


Fig. 8.9 Prototype PCB of DecRel tag

8.5.1.1 Analog Circuit

In this design, analog circuitry is used in both the relay path and the sensing path. The relay tag needs to use envelope detection technology to detect the envelope of the high-frequency signals, so it needs to design an envelope detector. As shown in Fig. 8.6, the envelope detector consists of a rectifier circuit and a low-pass filter. The rectifier circuit consists of two diodes in reverse parallel, which can improve the sensitivity and range. A P2D SCR thyristor is used. The output of the rectifier circuit is connected to a low pass filter consisting of a 10 k Ohms resistor and a 1 nF capacitor. The envelope detector also sets a threshold voltage of 0.3 V to distinguish between high and low voltages to eliminate noise and boost the voltage for FPGA modules. A TLV3501 with a 4.5 ns propagation delay is selected as the voltage comparator. The envelope detector can operate at frequencies up to 3200 MHz and has an antenna gain of 3 dBi. Its frequency range is 824 MHz to 960 MHz and 1710 MHz to 1990 MHz.

In the sensing path, we use discrete components and analog devices to build analog circuits, as shown in Fig. 8.5b. There are three types of analog sensing front-end, including microphone, photoresistor, and thermistor. The output is connected to a PWM baseband circuit. TLV3501 is selected as the voltage comparator, and 10k Ohms resistor and 100 nF capacitor are used in the RC calculator.

8.5.1.2 FPGA Circuit

We implement all digital logic circuits in FPGA. Verilog is used to specify the logic functions. The key to backscatter communication is tag modulation. For analog and

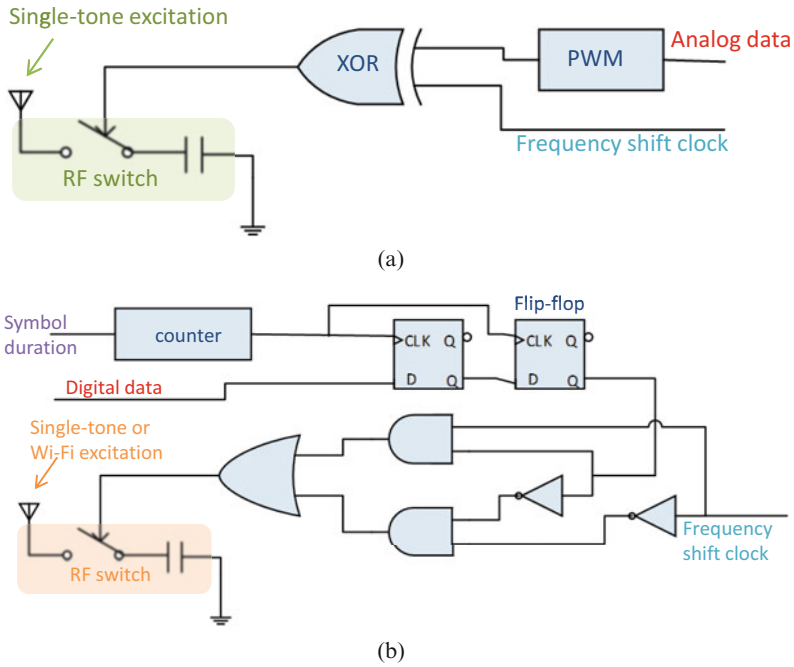


Fig. 8.10 Two circuits for tag modulation. (**a**) Analog data tag modulation. (**b**) Digital data tag modulation

digital baseband signals, we have developed appropriate tag modulation schemes. it is shown in Fig. 8.10.

In the tag modulation of the analog baseband, the analog baseband signal and the frequency shift clock signal generate an output signal by XOR to directly control the ADG902 RF switch. It is shown in Fig. 8.10a. The frequency of the output signal is the same as that of the frequency shift clock signal. The phase difference between the output signal and the pulse PWM signal is 0°. And the phase difference between the output signal and the interval PWM signal is 180°.

In the multi-hop backscatter sensor mesh, when the distance between nodes is long, the signal transmission path is also complex, so the transmission process will be affected by channel fading and multipath effects, and the signal may be attenuated and distorted. To solve this problem, digital baseband signals usually use time-based modulation technology, that is, to transmit data by specifying the fixed duration of high voltage and low voltage for each data bit. Figure 8.10b shows a tag modulation circuit based on a digital baseband signal. We can use counter blocks to control the duration of symbols. For monophonic excitation, we use the envelope detection pulse width to calculate the symbol duration. Specifically, we can use a counter block to count the width of the envelope detection pulse. We can express high level as '1' and low level as '0'. Tag modulation uses the rising edge of the first detection pulse to synchronize to a single-tone excitation signal.

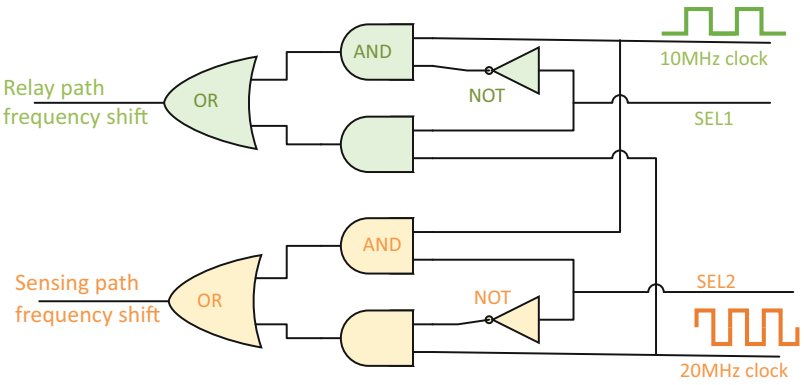


Fig. 8.11 Sensing path frequency shift selection and relay path frequency shift selection

To use Wi-Fi stimulation, we must first define the duration of the symbol. The duration T of each symbol is assumed to be one 802.11b bit or four 802.11g/n OFDM symbols [33, 34]. Then we can use a counter block to calculate the number of clock cycles. If the counter reaches a threshold, it will send a high level pulse, otherwise it will send a low level pulse. Similarly, high level can be represented by 1 and low level by 0. In label modulation, if the register outputs 1, the modulation outputs a 0° phase shift signal, otherwise a 180° phase shift signal is output. The tag cannot decode the Wi-Fi signal, so Wi-Fi excitation can only be used for the last hop tag. The modulation uses an external power amplifier detector (such as a 40 mW AD8313) to synchronize with the start of the Wi-Fi excitation packet.

We also proposed the use of frequency shift technology to make the sensing path and relay path of backscatter tags not interfere with each other. To realize frequency shift, the tag needs to set the corresponding clock signal and clock selection mechanism. We use the internal 50 MHz clock of XC3S500E FPGA to generate a 10 MHz clock. The verilog code of frequency division generates a 20 MHz clock. The clock selector can receive the clock from an input signal and route it to one of two different output channels. The relevant FPGA circuit is shown in Fig. 8.11.

The aggregation node will use certain modulation techniques, such as BPSK modulation, to send 8-bit control messages to the tag via the tone carrier. Therefore, the tag can recover the control message via the envelope detector and input it into a shift register for processing. Figure 8.12 shows the FPGA control message interpretation circuit and the corresponding on/off circuit module. The control message includes the ID used to specify the target tag, the bit used to control the tag to switch between the decodable relay and the analogue forwarding, and the bit used to select the baseband circuit or the frequency shift clock. The ID matching circuit of each tag is unique. If the ID matches, the circuit will output '1' to enable subsequent configuration, otherwise output '0' to ignore the message. In addition,

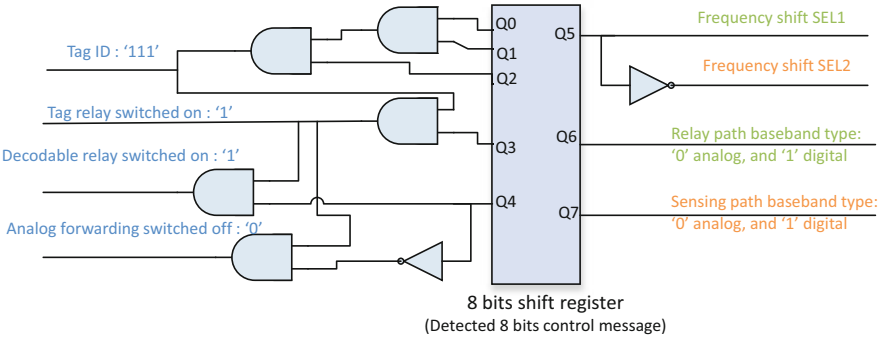


Fig. 8.12 FPGA circuits for interpreting the control message and switching on or off different tag configurations

the relay mode of the tag can be switched by the control bit. Note that the backscatter tag can only be reconfigured by nearby aggregation nodes.

8.5.1.3 Other Nodes

In the design, the radio equipment defined by the USRP N210 software is used to implement backscatter readers, excitation sources and aggregation nodes. We also use the Qualcomm AR938x device to realize the Wi-Fi excitation and receiver. The RFMAX S9028PCR antenna is used for excitation and its gain is 8.5 dBic. The reader and the aggregation node use the MTI 6.5 dBic MT-242025/TRH/A antenna. The excitation node and the sink node use different carrier center frequencies to avoid interference between multi-hop tags.

8.5.1.4 PCB and IC Performance Measurement

We use the PCB to verify the relevant indicators of the tags. Solar panels power the circuit. The monitor power monitor FTA22D [35] is used to check the power consumption. The data shows that the average power consumption in the idle state is 107.3 mW and that in the working state is 273.5 mW. To optimize the power consumption, we simulate the design in the IC design platform: use Cadence IC 6.17 Virtuoso to implement and evaluate analog components [36], and use TSMC 65 nm CMOS low-power technology library. We also use the Xilinx X Power analysis tool to synthesize digital components. We can find that the total power consumption of the label designed by IC is 337.9 μW. And the total power consumption of the label designed by PCB is 273.5 mW. IC design works better. Compared with X-Tandem [14], DecRel greatly reduces the power consumption of the frequency shifting.

8.5.2 Evaluation

In order to evaluate the performance of DecRel, we designed three sets of experiments and recorded some indicators, such as received signal strength index (RSSI), bit error rate (BER), throughput and signal to noise ratio (SNR). At the same time, in order to explore the scale that affects the network size, we checked the multi-hop communication range and the distance between tags.

When setting up the topology, we follow the following sequence: place the aggregation node at a maximum distance of 1 m from the DecRel tags. The distance between tags varies from 1.2 m to 4.8 m.We measure the effect of the number of hops on the bit error rate by increasing the number of tags by fixing the tag distance. We measure the distance from the last hop tag to the reader by fixing the tag and aggregation node positions and changing the reader position. For Wi-Fi motivation, we gradually increase the distance from 1 m to 12 m and for monophonic excitation, we gradually increase the distance from 1 m to 5 m.

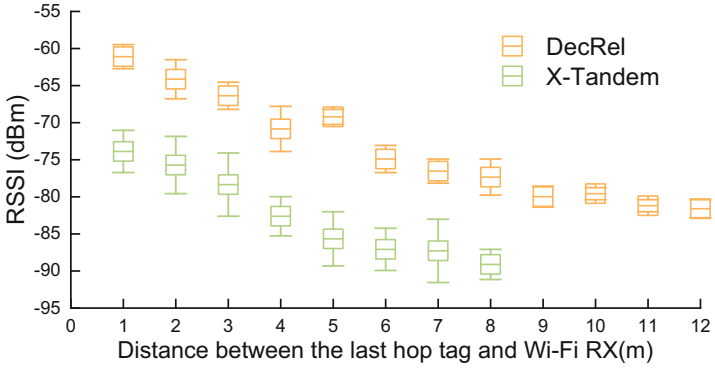
8.5.2.1 Performance of Digital Baseband and Modulation Circuits

We design the first experiment to evaluate DecRel when using digital baseband and digital data modulation circuits. As the previous multi-hop backscatter communication, X-Tandem [14] uses digital modulation and Wi-Fi stimulus signals. To better compare DecRel and X-Tandem, we make the last hop tag in DecRel use Wi-Fi.

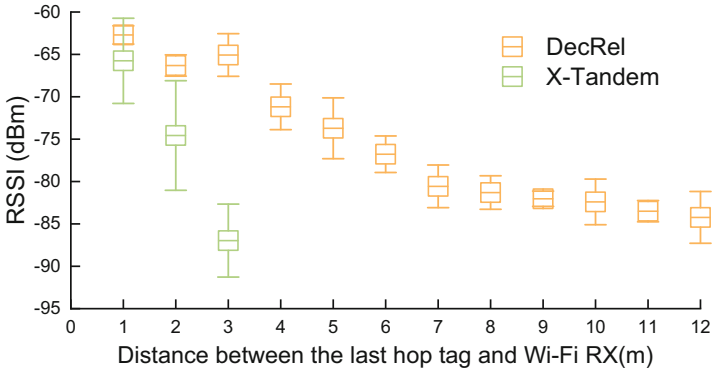
First, we deploy a multi-hop backscatter network to explore BER and hops. When the distance between tags is fixed at 1 m and the number of hops increases from 2 to 6, the BER decreases from 0.037 to 0.185. When the detected distance is fixed at 2 m and the number of hops increases from 2 to 6, the BER decreases from 0.066 to 0.341.

In addition, we refer to X-Tandem, the hops number of the backscatter network is 2, and investigate the effect of the distance between the last hop tag and the reader on the communication quality. We move the reader and assume the distance between the reader and the last hop tag is 1 m. At the same time, we configured three types of Wi-Fi excitation signals for experiments. As shown in Fig. 8.13, the received signal strength of DecRel and X-Tandem decreases with the increase of distance under three types of Wi-Fi excitation. When the detected distance is 1 m, the signal strength of the last hop of DecRel under three kinds of excitation is about 60 dBm.When the distance increases to 12 m, the signal strength decreases to below −80 dBm. However, in each case, DecRel is superior to X-Tandem in terms of signal strength and communication range of the last hop. It can be seen that jump attenuation does not significantly affect DecRel. This is because the intensity of the backscattered signal of the last hop of DecRel is not influenced by the signal of the previous hop.

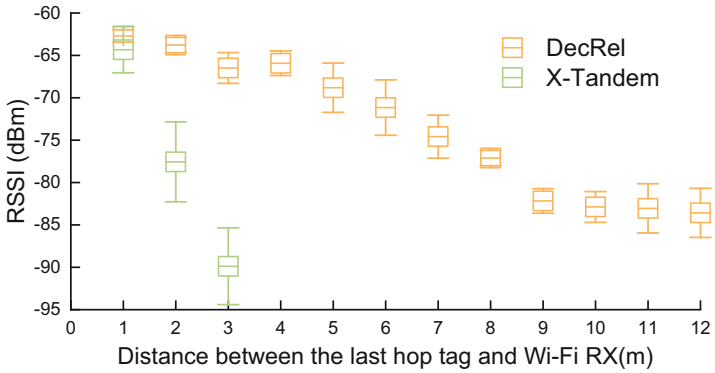
We also investigate the effect of the last hop distance on the BER and throughput of the last hop backscattered signal. As shown in Fig. 8.14, our design achieves a



(a)

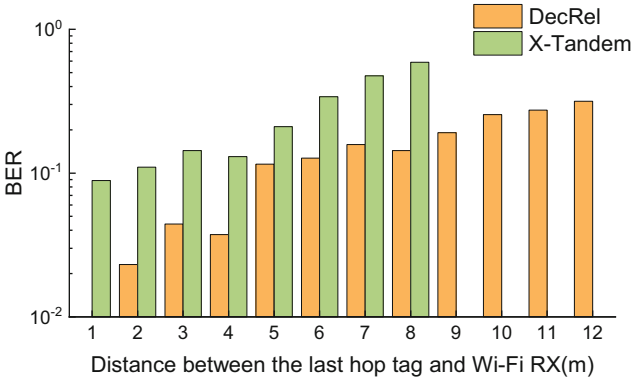


(b)

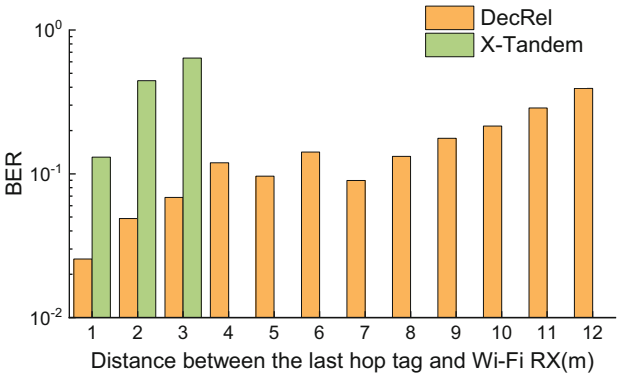


(c)

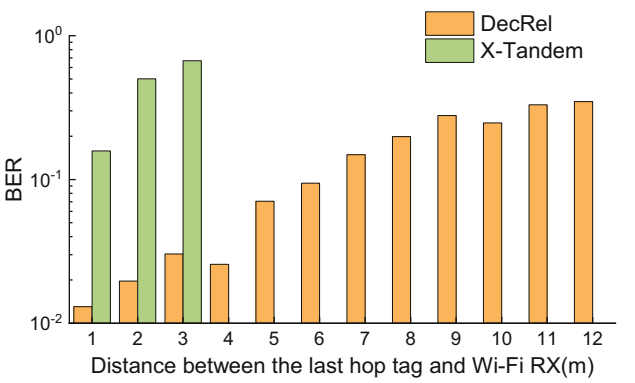
Fig. 8.13 The strength of the last hop backscattered signal across the distance between the last hop tag and Wi-Fi receiver. (**a**) 802.11b 1 Mbps. (**b**) 802.11g 6 Mbps. (**c**) 802.11n 6.5 Mbps



(a)



(b)



(c)

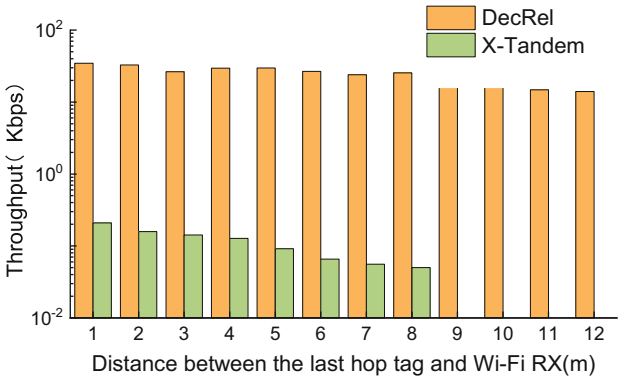
Fig. 8.14 The BER of the last hop backscattered signal across the distance between the last hop tag and Wi-Fi receiver. (**a**) 802.11b 1 Mbps. (**b**) 802.11g 6 Mbps. (**c**) 802.11n 6.5 Mbps

better BER than X-Tandem for different excitation specifications. When the distance between Wi-Fi receiver and the last hop is 1 m, the BER is an order of magnitude better than that of X-Tandem. And when we use 802.11g and 802.11n stimulation, X-Tandem with a distance of 3 m between the receiver and the last hop tag is higher than DecRel with a distance of 12 m between the receiver and the last hop tag. For different Wi-Fi stimulation, the throughput of DecRel is also better than that of X-Tandem,as shown in Fig. 8.15. In particular, when the Wi-Fi receiver is 1 m away from the last hop tag, DecRel can achieve multi-hop throughput of 35.1 Kbps, 32.6 Kbps and 33.0 Kbps under three types of stimulation, respectively. This is about 150 times higher than the level of X-Tandem in the same situation. When the last hop distance is increased to 12 m, the multi-hop throughput of DecRel is much better than that of X-Tandem. These results clearly prove that the analogue transmission mode of X-Tandem has strict signal attenuation, while DecRel has a good improvement on the backscatter signal strength of the last hop.

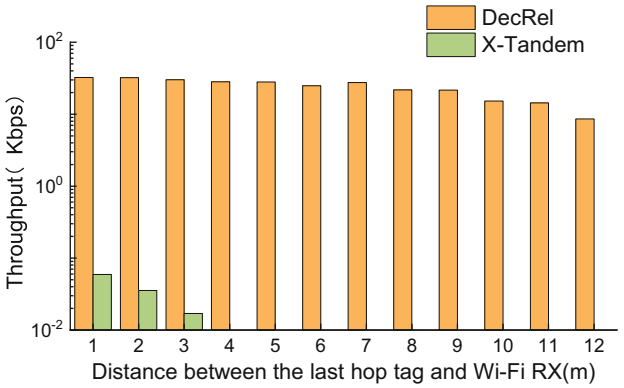
Since DecRel can choose to use Wi-Fi excitation and single-tone excitation in the communication of the last hop, we tested the performance under the two types of excitation respectively. The distance between the tag and the tag is still fixed at 1 m, and the distance between the last hop tag and the reader-writer gradually increases from 1 m. For single-tone excitation, we use the USRP N210 device as the reader. The experiment data are shown in Fig. 8.16. We can see that when the distance between the last hop tag and the reader-writer is changed, the use of Wi-Fi excitation is better than the case of single tone in terms of RSSI and BER. In terms of throughput, when the distance is 1 m, the single-tone condition outperforms the Wi-Fi condition. However, with the increase of the last hop distance, the throughput of the single-tone excitation decreases faster, and the Wi-Fi excitation is more stable. DecRel still has some advantages over previous works under the single-tone excitation. For example, its peak throughput is 200 times higher than that of X-Tandem, and single-tone excitation can be used for any jump, while Wi-Fi excitation can only be used for the last hop tag.

The communication range of a multi-hop backscatter sensor network is determined by the maximum distance between the first hop tag and the reader. The maximum distance is equal to the sum of the distance between the multiple tags and the tags and the distance between the last hop tag and the reader.The communication range of X-Tandem is typically about 8 m. The communication range is limited for two reasons. Firstly, the X-Tandem tag cannot be decoded and only the first-hop excitation is used. Secondly, the distance between X-Tandem tags is up to 0.4 m, which is negligible compared to the last hop distance of up to 8 m. Unlike X-Tandem, each tag in the DecRel system can use a distributed excitation signal independent of its previous hop excitation, which greatly increases the distance between tags. Therefore, as the number of tags increases, the communication distance of DecRel increases significantly.

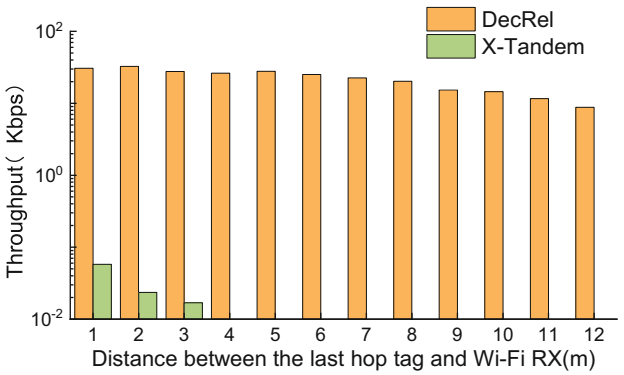
We also investigate the effect of the tag-to-tag distance on DecRel in the backscatter network with a hop number of 2. In the experiment, we fixed the distance between the last hop tag and the reader at 1 m and moved the position of the first hop tag to increase the distance between the tag and the tag to check the fingers,



(a)

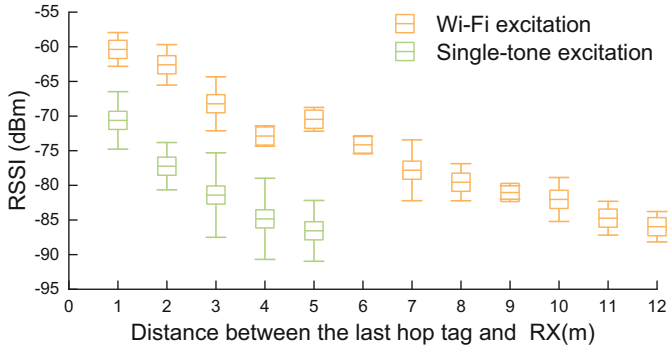


(b)

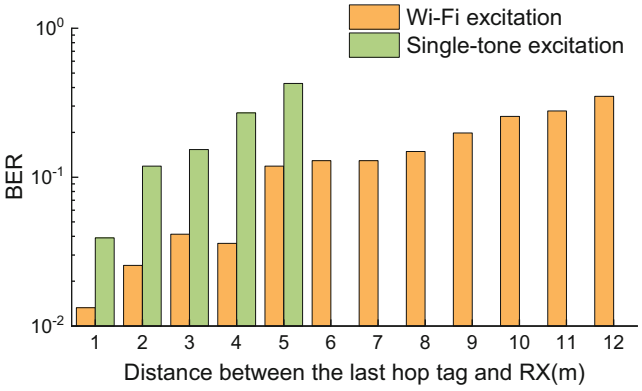


(c)

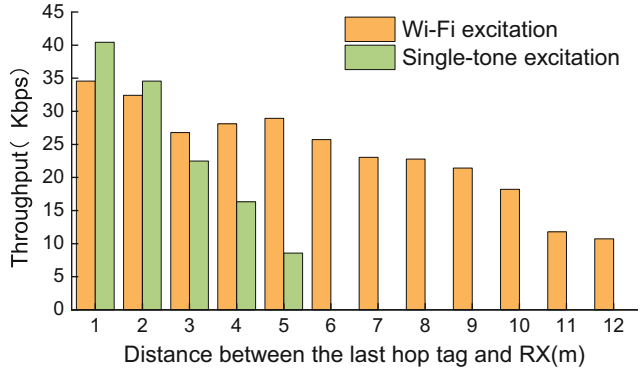
Fig. 8.15 The throughput of the last hop backscattered signal across the distance between the last hop tag and Wi-Fi receiver. (**a**) 802.11b 1 Mbps. (**b**) 802.11g 6 Mbps. (**c**) 802.11n 6.5 Mbps



(a)



(b)



(c)

Fig. 8.16 DecRel communication performance using digital baseband circuits under two excitations. (**a**) RSSI. (**b**) BER. (**c**) Throughput

such as RSSI, BER and throughput. To avoid bias caused by excitation, we detect these indicators under the conditions of single-tone excitation and Wi-Fi excitation respectively. Figure 8.17a shows that changing the distance between tags has little effect on the average RSSI under the two types of excitation. This is because each tag in the DecRel system uses a separate excitation signal. Figure 8.17b and c show the effect of the distance between tags on the bit error rate and throughput under two types of excitation. As the distance increases, the bit error rate of the relay increases significantly. According to the experimental setup, we only moved the position of the first hop tag to increase the distance between tags. The first hop tag is moved far away and the distance between it and the aggregation node is increased. This will result in a worse bit error rate. The worse bit error rate will indirectly affect the data transmission between the last hop tag and the reader.

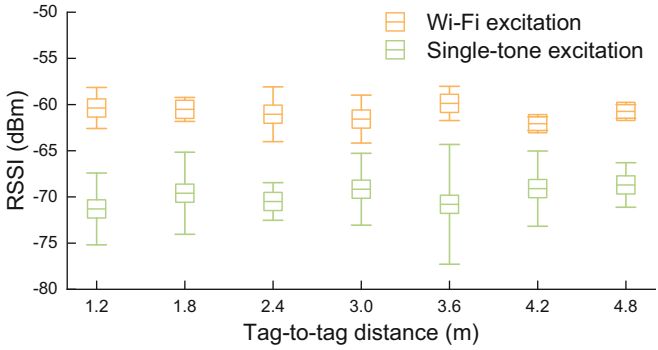
8.5.2.2 Performance of Analog Baseband and Modulation Circuits

Through experiments, we evaluate the performance of the analogue baseband and modulation circuits and obtain relevant data as shown in Fig. 8.18. We find that when the distance between tags is fixed at 1.6 m and 4.8 m, as the distance between the last hop tag and the reader increases from 1 m to 5 m, the three types of sensor circuits achieve similar signal-to-noise ratios, and the signal-to-noise ratio of the last hop backscattered signal decreases from about 35 dB to about 15 dB. It can be seen that the distance between tags does not affect the signal-to-noise ratio from the last hop tag to the reader.

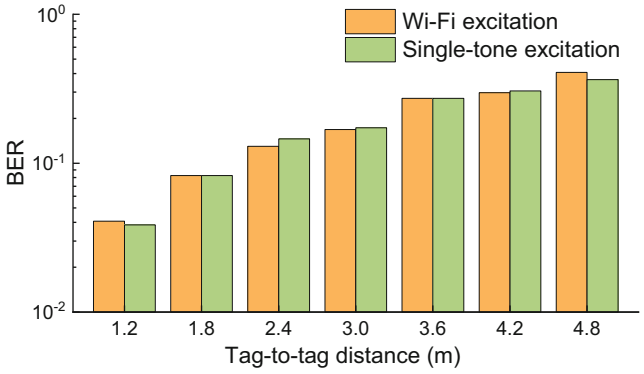
The analogue baseband has a sampling rate of 48 kHz when transmitting audio signals. When 16-bit quantization is used in the reader, this corresponds to a bit rate of 768 kbps, which is much higher than the digital baseband bit rate of 40 kbps. Figure 8.19 shows that the analogue baseband and digital baseband have similar signal-to-noise ratios. This is because the analogue baseband uses a PWM signal, and one pulse width can transmit more bits of information than the digital baseband. Since the analogue baseband circuit does not require external sensors, the power consumption of the tag is also greatly reduced.

8.5.2.3 SNR of Simultaneous Sensing and Relay

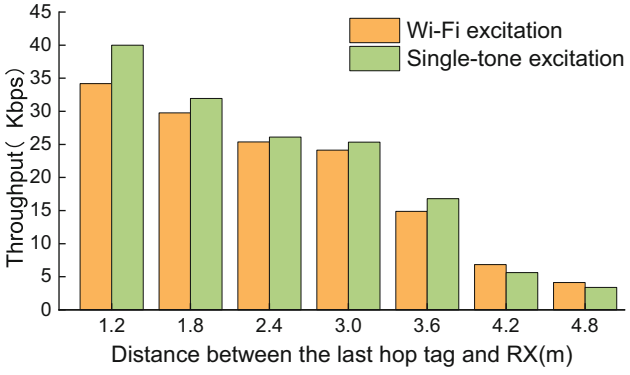
At the same time, we designed an experiment to verify it. As shown in Fig. 8.20, the first hop tag's sensing path, the second hop tag's relay path and the sensing path have similar SNRs, so the simultaneous multi-hop communication is almost undisturbed.



(a)



(b)



(c)

Fig. 8.17 Two hop backscatter performance across tag-to-tag distance using digital baseband circuits. (**a**) RSSI. (**b**) BER. (**c**) Throughput

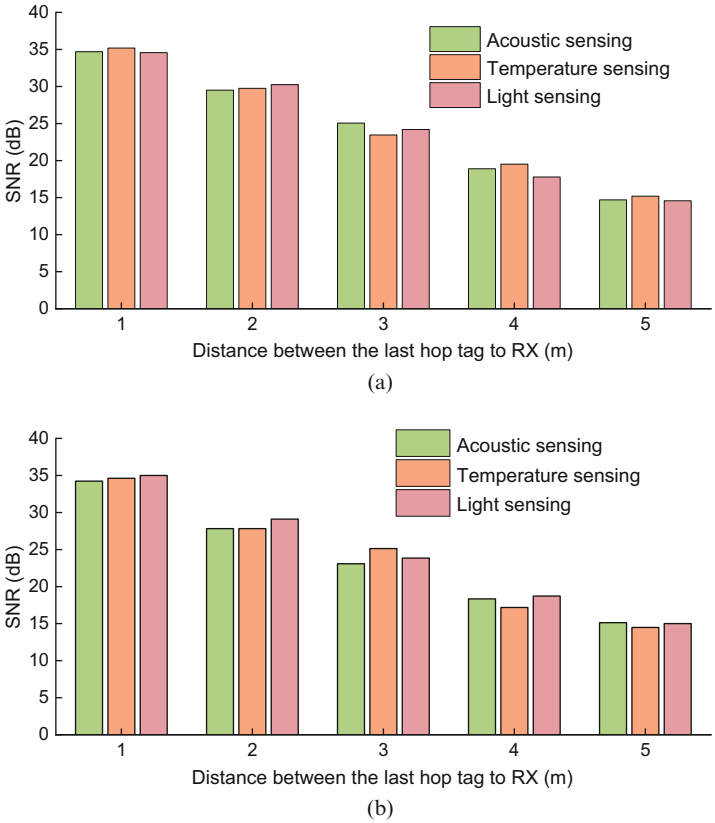


Fig. 8.18 The last hop backscattered signal quality of DecRel 48 kHz analog baseband and modulation circuits. (**a**) 1.6 m tag-to-tag distance. (**b**) 4.8 m tag-to-tag distance

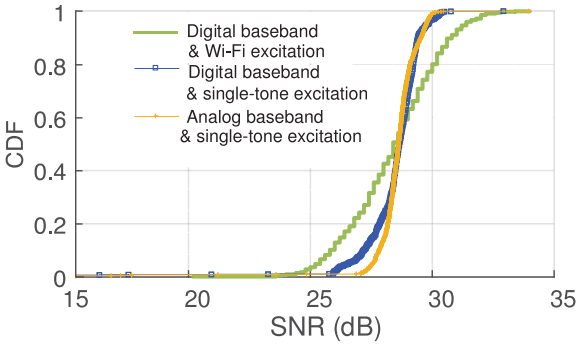


Fig. 8.19 SNR of DecRel with different baseband circuits

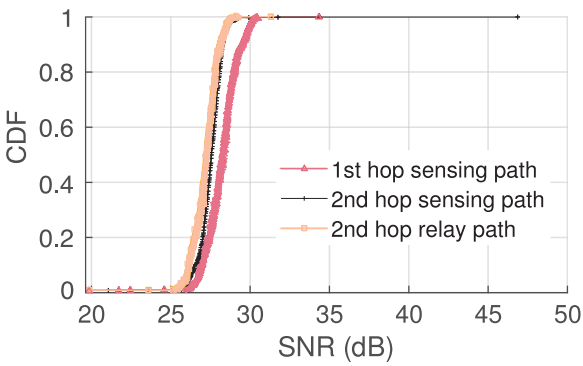


Fig. 8.20 SNR of DecRel when performing simultaneous sensing and relay

8.6 Application Case

From the above experiments, we can see that DecRel has obvious advantages, and the advantages are more obvious under the stimulation of Wi-Fi. Based on the above results, we propose that DecRel has certain potential applications in the construction of smart hospitals. Here, we will introduce two application scenarios in detail.

8.6.1 Location Management

Medical services are complex and busy, so it is necessary to follow up to ensure that patients are treated on time. The traditional positioning system in the hospital is based on RFID, such as Tagoram, which places readers in the corridor. When a nurse with a tag passes by, the reader reads the tag information and judges the direction. However, the positioning accuracy of RFID is greatly affected by the environment, such as metal, water, concrete and other materials that interfere with signal transmission, resulting in a decrease in positioning accuracy. In addition, RFID technology is sensitive to the position and orientation of tags, and the position or orientation deviation of tags will lead to inaccurate positioning. The cost of RFID technology is high. Factors such as the cost of manufacturing tags, the price of tag readers and writers, and the cost of software development will increase the overall cost of using RFID technology.

DecRel can further improve the tracking technology at a low cost and build a more powerful management system for doctors and nurses. Due to the popularity of Wi-Fi infrastructure, most hospitals have achieved full coverage of wireless networks. We just need to install sensors in the hospital, and these sensors can receive Wi-Fi signals in the hospital. Sensors should be placed in rooms, floors and corridors of hospitals. Relay tags are attached to the scrubs of doctors and nurses. When doctors and nurses enter the coverage area, the sensor can use the position measurement algorithm to calculate the positions of doctors and nurses and

send the backscattered signals back to the base station by reading the tags. The backscattered signal from the sensor can be used to calculate the position of doctors and nurses using the time difference measurement algorithm or the angle difference measurement algorithm. By combining these algorithms with the sensor data, the positioning accuracy can be improved.

In this application scenario, the system is beneficial to help patients contact the nearest medical staff at the first time, so that patients can receive first aid at the first time and ensure the safety of patients' lives. It can be widely used in hospitals.

8.6.2 Patient Information Monitoring

In hospitals, in order to provide better treatment, doctors need to be constantly informed about their patients' conditions. Traditionally, doctors obtain patient information by interviewing patients or compiling treatment records. However, this approach is inefficient and error-prone. Multi-hop backscatter sensor networks can provide an effective solution.

In a hospital, we can deploy tags with sensors on or around a patient's body. The sensors would sense physiological information such as heart rate, blood pressure, temperature etc. in real time. Nodes in the sensor network can feed the sensor information to neighbouring nodes, forming a wireless sensor network. And the nodes in a multi-hop backscatter sensor network can not only transmit information to the target nodes but also communicate with each other, which guarantees the communication quality and range of the sensor network. Therefore, multiple nodes can be deployed in different areas of the hospital to form a global network that can achieve comprehensive monitoring of patient information. As we have seen through previous experimental results, the multiple backscatter sensor network is highly stable and resistant to interference. We therefore believe that it can operate stably in complex hospital environments. And if a multi-backscatter sensor network is deployed in a smart hospital, this will help the hospital to provide long-term, real-time wireless monitoring, greatly improving the efficiency of the hospital and the safety of patients.

8.7 Summary

In this paper we have designed a multi-hop backscatter sensor mesh, DecRel. It is an innovative sensor architecture. In the design, we use distributed excitation. And to test the bias due to different excitations. We also used monophonic excitation and Wi-Fi excitation in our experiments. The experimental results show that the distributed excitation allows DecRel to no longer be limited to the distance between the tag and the excitation. The communication range increases to multiple tag-to-tag

distances. The backscattered sensor network using distributed excitation has a better transmission range.

At the same time we use decodable tag relay technology and frequency shifting technology. When sensing and relaying tasks are performed simultaneously, their transmission paths are deployed on two frequencies. This avoids interference between the sensing and relaying paths. Decodable tag relay technology greatly improves the quality of backscatter communication in sensor networks.

In application scenarios where we expect the design to be used for localization, the distributed excitation and decodable tag relay help us to obtain a larger communication range and better communication quality. In order to save energy, we have also designed a method to choose not to relay the code depending on the mobility of the tag. However, in this method, we need to reconfigure the tag by sending a control message. How to enable adaptive tag configuration based on mobility is a question we will need to think about later.

References

1. Memon ML, Saxena N, Roy A, Shin D-R (2019) Backscatter communications: Inception of the battery-free era—a comprehensive survey. Electronics
2. Li S, Xu L, Zhao S (2015) The internet of things: a survey. Inf Syst Front 17:243–259
3. Katti S, Katabi D, Balakrishnan H, Médard M (2008) Symbol-level network coding for wireless mesh networks. In: Conference on applications, technologies, architectures, and protocols for computer communication
4. Heinzelman WB, Kulik J, Balakrishnan H (1999) Adaptive protocols for information dissemination in wireless sensor networks. In: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking
5. Zorzi M, Rao RR (2003) Geographic random forwarding (geraf) for ad hoc and sensor networks: Energy and latency performance. IEEE Trans Mob Comput 2:349–365
6. Roundy S, Wright PK, Rabaey JM (2003) A study of low level vibrations as a power source for wireless sensor nodes. Comput Commun 26:1131–1144
7. Polastre J, Hill JL, Culler DE (2004) Versatile low power media access for wireless sensor networks. In: ACM international conference on embedded networked sensor systems
8. Gollakota S, Reynolds MS, Smith JR, Wetherall D (2014) The emergence of rf-powered computing. Computer 47:32–39
9. Bharadia D, Joshi KR, Kotaru M, Katti S (2015) Backfi: High throughput wifi backscatter. In: Proceedings of the 2015 ACM conference on special interest group on data communication
10. Liu V, Parks AN, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. In: Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM
11. Zhang P, Hu P, Pasikanti V, Ganesan D (2014) Ekhonet: high speed ultra low-power backscatter for next generation sensors. In: Proceedings of the 20th annual international conference on Mobile computing and networking
12. Talla V, Lindsay Smith JR (2013) Hybrid analog-digital backscatter: a new approach for battery-free sensing. In: 2013 IEEE international conference on RFID (RFID), pp 74–81
13. Jang J, Adib FM (2019) Underwater backscatter networking. In: Proceedings of the ACM special interest group on data communication
14. Zhao J, Gong W, Liu J (2018) X-tandem: Towards multi-hop backscatter communication with commodity wifi. In: Proceedings of the 24th annual international conference on mobile computing and networking

15. Wang J, Adib FM, Knepper RA, Katabi D, Rus D (2013) Rf-compass: robot object manipulation using rfids. In: Proceedings of the 19th annual international conference on mobile computing & networking
16. Wang J, Hassanieh H, Katabi D, Indyk P (2012) Efficient and reliable low-power backscatter networks. In: CCRV
17. Yeager DJ, Sample AP, Smith JR (2017) Wisp: a passively powered uhf rfid tag with sensing and computation. In: RFID Handbook. CRC Press, pp 261–276
18. Park S, Min C, Cho S (2009) A 95nw ring oscillator-based temperature sensor for rfid tags in 0.13 μm cmos. In: 2009 IEEE international symposium on circuits and systems, pp 1153–1156
19. Roy S, Jandhyala V, Smith JR, Wetherall D, Otis BP, Chakraborty R, Buettner M, Yeager DJ, Ko Y-C, Sample AP (2010) Rfid: From supply chains to sensor nets. Proc IEEE 98:1583–1592
20. Johan S, Zeng X, Unander T, Koptyug A, Nilsson H-E (2007) Remote moisture sensing utilizing ordinary rfid tags. 2007 IEEE Sensors, pp 308–311
21. Bhattacharyya R, Floerkemeier C, Sarma SE (2010) Low-cost, ubiquitous rfid-tag-antenna-based sensing. Proc IEEE 98:1593–1600
22. Luo Z, Zhang Q, Ma Y, Singh M, Adib FM (2019) 3d backscatter localization for fine-grained robotics. In: Symposium on networked systems design and implementation
23. Airffnder (2018) A breakdown of 7 rfid costs, from hardware to implementation. https://www.airffnder.com/blog/rffd-cost
24. Iyer V, Talla V, Kellogg B, Gollakota S, Smith JR (2016) Inter-technology backscatter: Towards internet connectivity for implanted devices. In: Proceedings of the 2016 ACM SIGCOMM conference
25. Naderiparizi S, Hessar M, Talla V, Gollakota S, Smith JR (2018) Towards battery-free hd video streaming. In: Symposium on networked systems design and implementation
26. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: Backscatter communication using commodity radios. In: Proceedings of the 13th international conference on emerging networking experiments and technologies
27. Eslami M, Karimi O, Khodadadi T (2014) A survey on wireless mesh networks: Architecture, specifications and challenges. In: 2014 IEEE 5th control and system graduate research colloquium, pp 219–222
28. Karthika JR (2016) Wireless mesh network: a survey. In: 2016 international conference on wireless communications, signal processing and networking (WiSPNET), pp 1966–1970
29. Kumata Y, Koyama A (2014) Mesh net viewer ii: an extended visualization system for wireless mesh networks. In: 2014 17th international conference on network-based information systems, pp 53–60
30. Zhao J, Gong W, Liu J (2020) Towards scalable backscatter sensor mesh with decodable relay and distributed excitation. In: Proceedings of the 18th international conference on mobile systems, applications, and services
31. Talla V, Kellogg B, Gollakota S, Smith JR (2017) Battery-free cellphone. In: Proceedings of the ACM on interactive, mobile, wearable and ubiquitous technologies 1:1–20
32. Zhang P, Bharadia D, Joshi KR, Katti S (2016) Hitchhike: Practical backscatter using commodity wifi. In: Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM
33. Abedi A, Dehbashi F, Mazaheri MH, Salehi-Abari O, Brecht T (2020) Witag: seamless wifi backscatter communication. In: Proceedings of the annual conference of the ACM special interest group on data communication on the applications, technologies, architectures, and protocols for computer communication
34. Xu X, Shen Y, Yang J, Xu C, Shen G, Chen G, Ni Y (2017) Passivevlc: enabling practical visible light backscatter communication for battery-free iot applications. In: Proceedings of the 23rd annual international conference on mobile computing and networking
35. FTA22D. https://www.msoon.com/lvpm-software-download
36. Cadence IC 6.17 413 Virtuoso. https://www.cadence.com/en_US/home/tools/custom-ic-analog-rfdesign

Chapter 9
Multiprotocol Backscatter with Commodity Radios

Abstract In Chaps. 7 and 8, we focus on multi-hop backscatter systems to build networks. However, to achieve the construction of a large-scale backscatter network, in addition to building a multi-hop network, it is also necessary to support multi-protocol access. In this chapter, we present multiscatter, a novel battery-free backscatter system that possesses the capability to operate concurrently with multiple excitation signals. In pursuit of this objective, we make three pivotal contributions. First, our research unveils for the first time that the backscatter tags have the ability to discern diverse excitation signals, such as Wi-Fi, Bluetooth, and ZigBee, in an exceptionally energy-efficient manner. In addition, we introduce a new modulation method called overlay modulation to enable a single personal radio to decode both the productive and tag data. Further, a low-power listening scheme is proposed to save power consumption, achieving an energy efficiency system. Considering the ubiquitous presence of 2.4 GHz signals including Wi-Fi, BLE and ZigBee, and personal radios in our daily lives, the multiscatter technology can be effortlessly integrated into various IoT applications, further emphasizing its practicality and potential. Comprehensive experimental results prove the effectiveness of our system. We can accurately identify four different signals (802.11b, 802.11n, ZigBee, and Bluetooth) with an average accuracy rate of 93%. Thanks to the design of overlay modulation, the maximal aggregate throughput of both data achieves 278.4 kbps when using Bluetooth as excitation. Moreover, it possesses the capability to harness the diversity of excitation signals, ensuring uninterrupted communication and enabling substantial gains in throughput. In contrast, when carrier signals become unavailable, the single-protocol tag remains idle.

9.1 Introduction

In the previous chapters, we have given a comprehensive overview of the backscatter system. It holds the remarkable ability to achieve ubiquitous connectivity upon ultra-low-power sensors [1–18]. Over the past decade, researchers in the field of backscatter communication have exerted tremendous efforts to explore and harness existing signals and commodity radios [4, 19–30]. Some of them are dedicated to

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_9

improving the throughput of the system, some focus on improving the pervasiveness of the system, and some are concerned with the compatibility of the system. On the basis of existing work, we envision the requirements that a generic backscatter system should satisfy:

1. *Universal:* In everyday life, there are many different types of signals, such as Wi-Fi, ZigBee, Bluetooth, LTE, LoRa, 5G, etc. The ideal backscatter system should be able to support a wide range of different protocols, which would then greatly increase the versatility of the system.
2. *Compatible:* Many existing backscatter systems use single-tone as the carrier, such non-productive signals are not common in life. Moreover, the specific carriers significantly diminish spectral efficiency, affecting transmission performance. Therefore, the desired system should permit excitation signals to serve as carriers for tag data while simultaneously transmitting their productive data.
3. *Deployable:* To facilitate seamless and widespread adoption, the system should possess the capability of single personal-radio decoding. Introducing additional hardware or firmware modifications would incur additional costs for personal IoT sensors, making simplicity and compatibility key factors in achieving widespread implementation.

Although the aforementioned requirements may appear straightforward, in reality, no existing backscatter system manages to fulfill all of them. Designing a backscatter system that simultaneously meets the three above requirements is still a significant challenge. In this chapter, we present a possible solution, multiscatter, that can satisfy all these requests as shown in Fig. 9.1. It first identifies the different protocols in a low-power way and then embeds the tag data on different carriers in

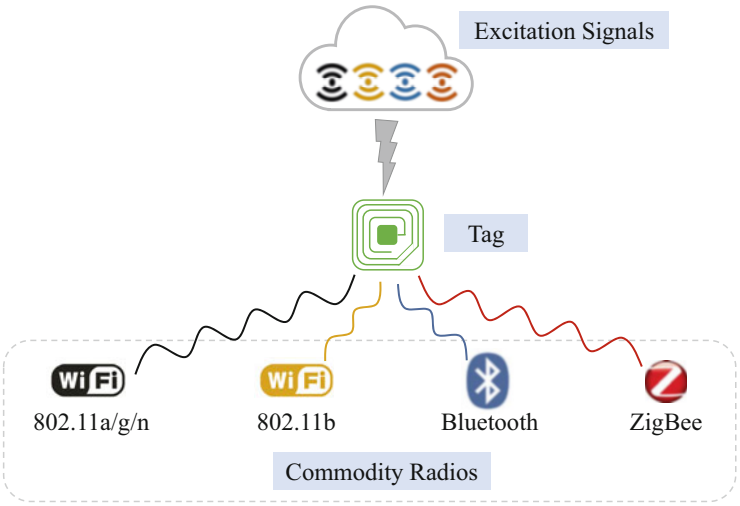


Fig. 9.1 Multiscatter conceptual design

different ways according to signal characteristics. At the receiver, both productive and tag data can be decoded simultaneously using only one AP. To achieve this goal, we still have three challenges to address.

1. How to Distinguish Different Excitation Packets?

In wireless communication, signal detection and identification are the two basic operations for data transmission. Designers have added some specific chips on the packets for signal identification, which are called preamble in most cases. Active devices achieve signal identification by using high power-consuming components like amplifiers, high-frequency oscillators to acquire high-bandwidth baseband signals and perform complex signal processing. However, limited by the low-power design of the tags, it is unavailable to use power-hungry components and has an extremely stringent constraint of computational complexity. Our solution is to design a high-bandwidth rectifier using simple hardware components such as diodes, capacitors, resistors, etc. We further use quantization, downsampling, and order matching to reduce computational overhead while maintaining high recognition accuracy. The details are shown in Sects. 9.3.2 and 9.3.3.

2. How to Perform Tag Modulation and Make Both Types of Data Decodable on a Single Commodity Radio?

Enabling productive carriers is an important step toward pervasive backscatter systems. However, existing state-of-the-art systems, including Hitchhike, X-Tandem, and PLoRa, are reliant on productive data within the original channel for successful tag data decoding. Consequently, in scenarios where the original productive data becomes corrupted, the recovery of tag data becomes impossible, even if the backscattered packets are right. To overcome this limitation, we propose a novel modulation approach called overlay modulation. We divide the payload into two parts: the reference data and the modulatable data, where the reference data is arbitrary and the modulatable data is a duplicate of the reference data. By embedding the tag only on the modulatable part, it is possible to carry both kinds of data on a single packet. By comparing the reference symbols against the modulated symbols, we can decode both productive and tag data with a single commodity radio. A detailed explanation is provided in Sect. 9.3.4.

3. How to Improve Energy Efficiency for Event-Driven Transmissions?

The backscatter system operates passively and is driven by the carrier wave. Therefore, the tag does not need to be working at full speed all the time leading to a waste of energy. Instead, it can remain dormant until the presence of excitation signals triggers its activation. To optimize the system's energy efficiency, we present a customized state machine that controls the tag's behavior in various scenarios. We design a new listening mode that can operate at much lower power consumption than the Rx and Tx modes. The detailed design is introduced in Sect. 9.3.5.

In summary, our main contributions are as follows:

- We are the first to support effective identification of multiprotocol, e.g., Wi-Fi (802.11b/n), Bluetooth, and ZigBee.

- We propose overlay modulation, a new modulation method that can carry two types of data on a single packet and demodulate it using a single commercial receiver. Also, this method offers remarkable flexibility in adjusting the tradeoffs between tag-data rates and productive-data rates.
- We present a customized state machine that adds a listening scheme to the event-driven backscatter system reducing power consumption.
- We successfully demonstrate the functionality of our system, showcasing its ability to harness multiple excitation signals and provide significantly enhanced connectivity in real-world scenarios. Extensive experiments validate the feasibility and efficacy of our system.

9.2 Related Work

In the wireless network community, the exploration of backscatter as a means of pervasive communication for IoT networks has remained a prominent and widely discussed topic over the past decade. Much of the previous work has already contributed a lot in different ways. Ambient backscatter [20] is the seminal work that enables device-to-device backscatter communication. FS backscatter [24] improves SNRs of the systems by frequency-shifting. Thanks to a dedicated plug-in device generating single-tones as carriers, Passive Wi-Fi [25] achieves up to 11 Mbps data rate. Hitchhike [28] turns productive backscatter a reality at the symbol-level due to codeword translation.

However, none of them can satisfy the three requirements mentioned in Sect. 9.1 for two main reasons. First, no previous work has explored how to identify different signals and exploit this diversity. The closest existing work in this domain is FreeRider [29], which offers a comprehensive approach to modulating multiple excitation signals including Wi-Fi, and Bluetooth. However, it does not encompass support for excitation signal identification. [31] proposes a backscatter modulation technique capable of accommodating multiple protocols. However, it is important to note that the tag itself lacks the ability to identify the excitation signals. Therefore, a software-defined radio (SDR) is necessary for tag data decoding. Second, they cannot decode both types of data with a single commercial receiver device while using productive data as a carrier and performing modulation at symbol-level. Wi-Fi backscatter [22] and FS backscatter are compatible but work at packet-level with a low data rate. Interscatter [21] and LoRa [27] enable a single commodity receiver but require specific single tones as carriers. On the other hand, Hitchhike [28], FreeRider [29], and X-Tandem [30] can utilize productive signals as carriers but need two receivers for tag data decoding. Precise synchronization between the two receivers is required. PLoRa [26] only supports the productive carriers. Table 9.1 illustrates the detailed comparison of state-of-the-art backscatter systems.

Table 9.1 Comparison of state-of-the-art backscatter systems

	Excitation diversity	Productive carrier	Single commodity receiver
Wi-Fi backscatter [22]		★	★
FS backscatter [24]		★	★
Interscatter [21]			★
Passive Wi-Fi [25]			★
Hitchhike [28]		★	
FreeRider [29]		★	
X-Tandem [30]		★	
Multiscatter [32, 33]	★	★	★

In the pursuit of advancing backscatter communication, [32, 33] builds upon and draws inspiration from the above works and proposes a novel solution that realizes a universal, compatible, and deployable backscatter system.

9.3 Multiscatter Design

In this section, we will describe the system design in detail. Firstly, we provide an overview of our multiscatter framework. After that, we explain how to acquire high-bandwidth baseband signals, which are used for protocol identification introduced next. We then present the overlay modulation that can embed tag data onto productive carriers. Finally, we discuss our approach to reducing the listening power.

9.3.1 Overview

The framework of multiscatter is shown in Fig. 9.2. The energy harvesting module in the tag is used to provide energy support for the system by collecting RF energy from the 2.4 GHz ISM band as well as light energy using solar panels. The system is waiting for carriers in a low-power mode by the listening module until the excitation signal comes. Then, the tag obtains the baseband signal by utilizing a high-bandwidth rectifier and identifies the type of incoming carrier by correlation. At the same time, we use a series of operations to reduce the computational complexity. Finally, the system selects the appropriate modulation scheme to embed the tag data onto the carriers.

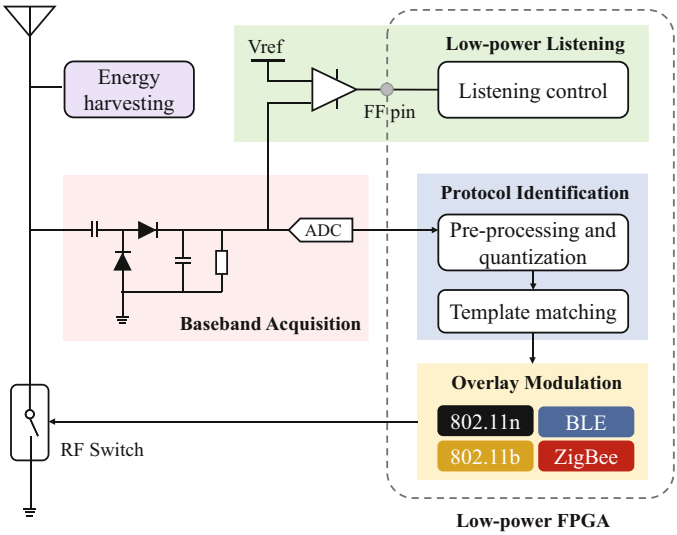


Fig. 9.2 Multiscatter overview

9.3.2 High-Bandwidth Signal Acquisition

For all wireless communication, packet detection is the first step for signal processing. In addition to indicating the arrival of a signal, the type of protocol is also identified during packet detection. Each protocol has a preamble at the beginning of a packet for signal recognition, which is unique for different protocols. For example, a typical 802.11b packet consists of a preamble lasting 144 μ s (128 scrambled 1's and 16 Start Frame Delimiter bits), and Bluetooth uses a preamble of 8 μs (0xAA). Active Radios can easily obtain high-quality signals with some high power-consuming components, but for tags, it is a great challenge to obtain high-bandwidth signals due to power consumption limitations. To solve this problem, we design a new envelope detector.

9.3.2.1 High-Bandwidth Envelope Detector

Firstly, we consider the envelope strength of obtained signals. Instead of using high-frequency mixers and low-noise amplifiers in active radios, we use a rectifier that is sensitive to signal energy to obtain baseband amplitude information. As shown in Fig. 9.3a, the basic rectifier is used as an "envelope detector" in RFID protocols. As the incoming signal's amplitude rises, the rectifying diode increases the voltage across the capacitor. Conversely, when the input amplitude decreases, the capacitor voltage decreases as it discharges through resistor R_1. In this way the absolute value of the baseband signal can be obtained, thus enabling a simple, cheap, and effective

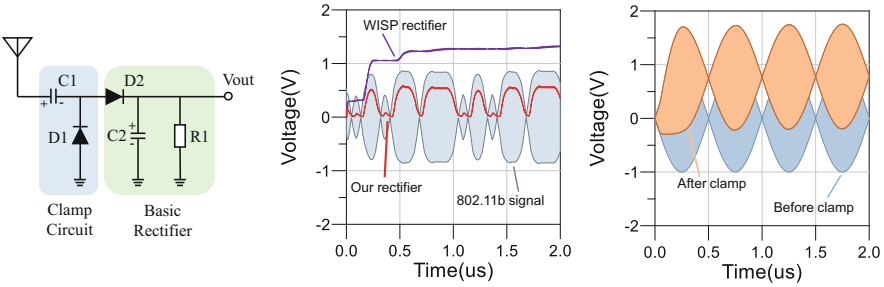


Fig. 9.3 High-bandwidth baseband signal. (**a**) Clamp circuit. (**b**) Clamp voltage booster. (**c**) Rectified signals

way of monitoring the signal envelope. However, the quality of the signal obtained by this circuit is not sufficient for our system. Therefore, we add a clamp circuit before the basic rectifier. They form a two-stage rectifier, which effectively increases the voltage of the acquired signal as shown in Fig. 9.3b. In this scenario, one might consider employing a multi-stage rectifier to achieve higher voltage. However, in contrast, a higher-stage rectifier reduces rectifying efficiency as well as distorts the signals.

Second, we delve into the response rate of the rectifier. Figure 9.3a demonstrates that the rectifier is made up of resistors, capacitors, and diodes. Therefore, the discharging speed of the capacitor τ greatly affects the quality of obtained baseband signals. τ, a time constant of an RC circuit, needs to be set at a proper value, otherwise, it will cause severe distortion of the signal. We denote the carrier frequency of input RF signals as f_c, and the corresponding baseband frequency is represented as f_b. The ideal value of τ should be $\frac{1}{f_c} \ll \tau \ll \frac{1}{f_b}$ [34]. $f_c = 2.4\,\text{GHz}$ since Wi-Fi, Bluetooth, and ZigBee can all operate at 2.4 GHz. We choose f_b as 20 MHz the bandwidth for Wi-Fi as that of Bluetooth and ZigBee are much lower. Figure 9.3c illustrates the comparison result between our rectifier and WISP rectifier [35] when using 802.11b as input signals. It is evident that the output signal for the WISP rectifier is largely distorted since it is designed for low-bandwidth signals (between 40 to 160 kbps for RFID readers). On the contrary, our rectifier performs significantly better with high-bandwidth input signals, owing to the precisely calibrated clamp and RC circuits.

9.3.2.2 Template Matching

Taking advantage of our newly designed rectifier, we can acquire high-bandwidth baseband signals for further protocol identification. All the obtained baseband signal envelopes are shown in Fig. 9.4. It is obvious that these four signals have their own characteristics and are distinguishable. The amplitude of the signal, the structure of

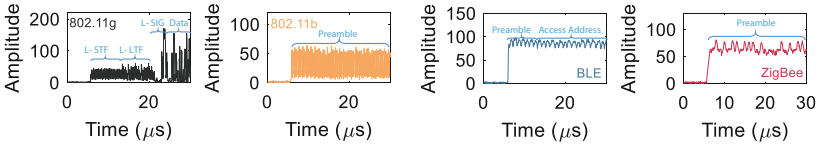
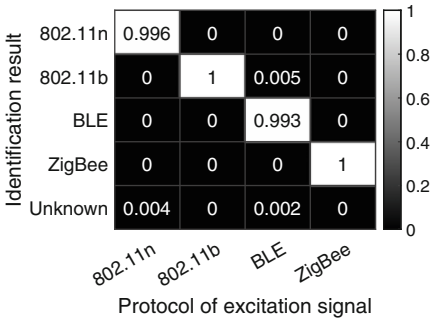


Fig. 9.4 Envelope shapes for four signals

Fig. 9.5 Identification accuracy



the signal, and the duration of the preamble vary significantly among these signals. Here, we use template matching for signal recognition. We determine the signal type by measuring the similarity between the input signal and the template by correlation calculations. First of all, we should set proper templates. The templates used in our systems contain two parts: a preprocessing window for DC removal and normalization, and a matching window for correlation computation. We define the length of the entire template to be L_t, where the length of the preprocessing window and the matching window are L_p and L_m, respectively, and $L_p + L_m \leq L_t$. These parameters can be set in a number of ways. Then, we use an ADC to sample baseband signals and test our system in the following settings. We choose the minimal length of preambles for four protocols, 8 μs, as the whole template window size, and the sampling rate is set at 20 Msps. In this manner, $L_t = 160$ samples. There are many combinations of L_p and L_m, and numerous experiments have shown that many combinations can achieve identification accuracy of over 99%. Figure 9.5 shows the case when $L_p = 40$ and $L_m = 120$. We can see that the average identification accuracy reaches 99.7% and all of them are over 99.3%. The results demonstrate that the baseband signals obtained from the four protocols are of high quality, making them well-suited for packet identification purposes.

9.3.3 Low-Power Protocol Identification

In the previous section, we demonstrate the feasibility of the protocol identification method when sufficient computational resources are available. However, the power consumption of our tag is limited to as low as 2 μW. Next, we show a series

Table 9.2 Comparison of computing resource usage for different FPGA implementations

	Multipliers needed	Adders needed	D-Flip-Flops needed
Each protocol	120	119	33,341
Total (Naive Impl.)	480	476	133,364
Nano FPGA Impl.			2860

of operations to reduce the computational complexity so that the multiprotocol identification algorithm can meet the power constraints.

9.3.3.1 Low-Power Computation

To understand why straightforward correlation-based matching is impractical for the tag, we show the required computational resources for the matching operation as shown in Table 9.2. When the matching template size is 120, it needs 120 multipliers and 119 adders to do correlation computation for each protocol identification. In FPGA, a 9*9 multiplier takes 259 D-Flip-Flops, and a 9*9 adder takes 19 D-Flip-Flops. The estimation reveals that a total of 133,364 D-Flip-Flops would be consumed for four protocols. However, we choose the FPGA, gloo nano AGLN250, which has the lowest power consumption to prototype our tag to meet the power constraints. Since AGLN250 has only 6144 D-Flip-Flops, the above algorithm will fail to work.

To tackle this challenge, we trade identification accuracy for meeting the ultra-low-power requirements of the FPGA. We use two operations in achieving this goal: quantization and downsampling [36–38]. Since multipliers consume more resources than adders, we first need to convert the multiplication operation into an addition. We quantize each sample into 1 bit reducing the D-Flip-Flops needed to about 2860 when the $L_m = 120$. At the same time, we reduce the sampling rate to 10 Msps to further reduce resource consumption. Figure 9.6a shows the identification results in this manner. We can see that the average accuracy is slightly lower than that in Fig. 9.5 but not too much. Therefore, quantization and downsampling effectively reduce computational resources while maintaining the accuracy of the protocol identification.

9.3.3.2 Ordered Matching

In the course of our experiments, we observe an interesting phenomenon: the resilience of the four protocols is different, which motivates us to do ordered matching. Figure 9.7a demonstrates that ZigBee signals can be identified first when the threshold is set as a similar value to ZigBee-template correlation. Similarly, Bluetooth, 802.11b, and 802.11n can be determined one after another as shown in Fig. 9.7a, b and c. Such a different signal resilience is mainly due to the different

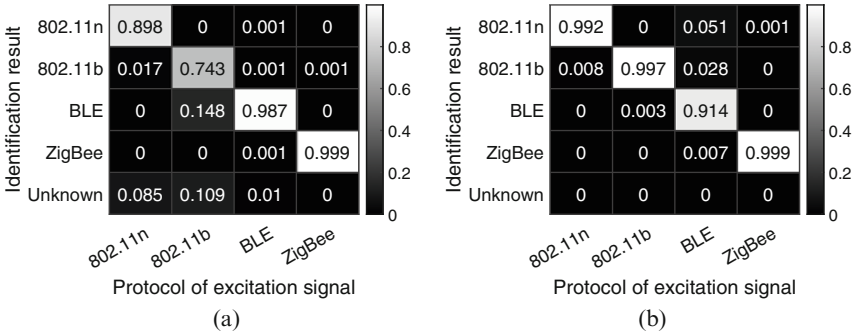


Fig. 9.6 Comparison of blind and ordered matching. (**a**) Blind matching at 10 Msps. (**b**) Ordered matching at 10 Msps

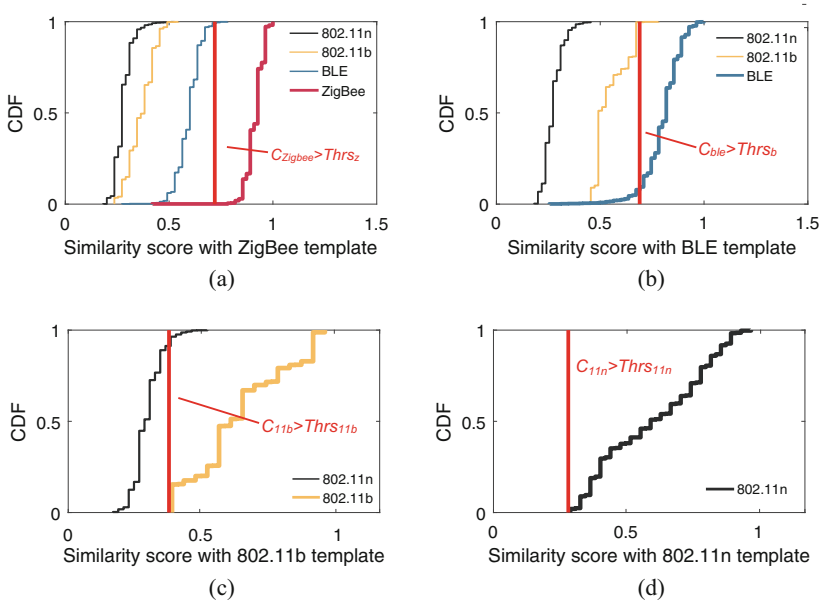


Fig. 9.7 Ordered matching, from ZigBee to BLE, to 802.11b, and 802.11n. (**a**) Step 1: $C_{ZigBee} > Thrs_z$. (**b**) Step 2: $C_{BLE} > Thrs_b$. (**c**) Step 3: $C_{801.11b} > Thrs_{11b}$. (**d**) Step 4: $C_{802.11n} > Thrs_{11n}$

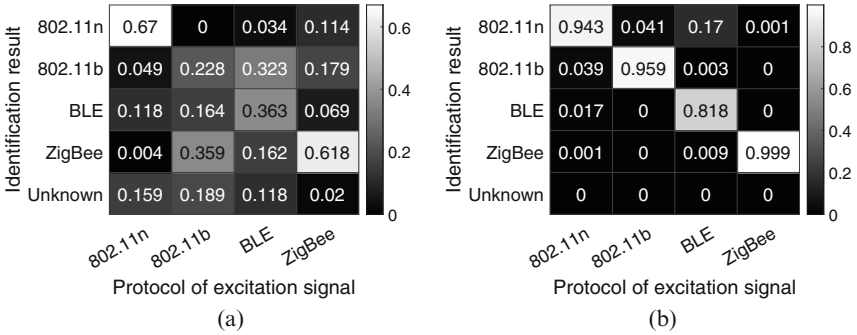


Fig. 9.8 Comparison of different matching windows. (**a**) 8 μs-matching window at 2.5 Msps. (**b**) 40 μs-matching window at 2.5 Msps

characteristics of the signal such as modulate scheme, symbol size, and modulation rate. This phenomenon is maintained when the sampling rate is reduced from 25 Msps to 10 Msps. Extensive experiments have been done to obtain the best parameter settings and statistical results. We conduct over 200,000 experiments in different ranges, scenarios, and protocols, all with consistent results. Compared with blind matching in Fig. 9.6a, the average identification accuracy increases from 0.906 to 0.976 as shown in Fig. 9.6b.

The advantage of ordered matching gives us the opportunity to reduce the sample rate even further. We try to find a lower bound for the sampling rate and Fig. 9.8a shows that the average recognition accuracy is only 0.485 when the sampling rate reduces to 2.5 Msps. Therefore, we intend to improve the performance by prolonging the length of the template. We need to find a template size that is suitable for all four protocols. 802.11b and ZigBee will not be a limitation for us as their preamble is over 100 μs. For BLE, the matching window size can be extended to 40 μs by including the fixed broadcasting address. Similarly, since there are HT-STF and HT-LTF fields lasting more than 20 μs after the legacy preamble, we can also set a matching window with 40 μs for 802.11n. Thanks to the window size extension, the average identification accuracy boosts from 0.485 to 0.93 as shown in Fig. 9.8b. We finally set the parameters to a sampling rate of 2.5 Msps and a window size of 40 μs.

9.3.4 Overlay Modulation

Now, we can identify the type of protocol accurately, we need to modulate the tag data onto the different carriers accordingly. Thanks to codeword translation [28], many state-of-the-art backscatter systems enable the use of productive data as a carrier. But they all face the same problem: two receivers are needed to capture the original data and backscatter data from two channels. When the original channel

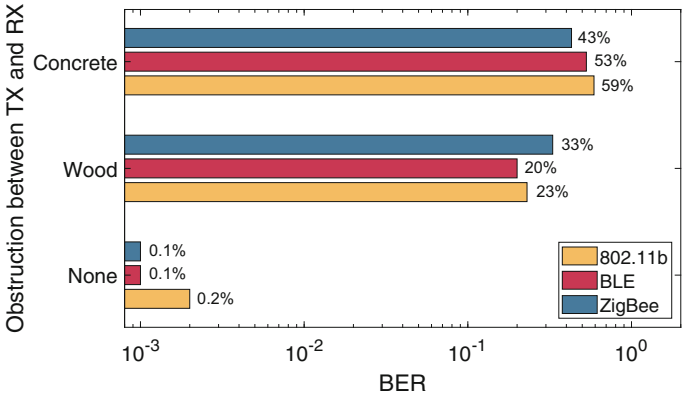


Fig. 9.9 BER increases rapidly when the original channel is occluded

encounters instability due to occlusion or mobility, decoding tag data becomes difficult, even if the data received through the backscattered channel is completely right. This highlights the strong dependence of tag-data decoding quality on the data from the original channel. We set up three scenarios to demonstrate this problem: the original channels with no obstruction, a wooden wall, and a concrete wall. Figure 9.9 shows that once the original channel is blocked, the BER rises rapidly from 0.2% to 59%. Therefore, to solve this problem, we propose a novel overlay modulation method enabling a single receiver for data decoding in this section.

9.3.4.1 Reference-Based Tag Modulation

Our goal is to be able to support a single commercial receiver while using productive signals as carriers and eliminate the need for data from two channels as in previous systems. Our key insight here is that the core of codeword translation is to use the original data as a reference, and that reference data and modulation data can exist in the same data packet. Inspired by the pilot symbols commonly used in wireless communication [39] and overlay networks built on top of existing networks, we propose a novel approach called reference-based overlay modulation. The workflow of overlay modulation is shown in Fig. 9.10. Every data packet is divided into groups with κ symbols and each group has two parts: a reference symbol and $\kappa - 1$ modulatable symbols. The modulatable symbols are exactly the same as the reference symbol. Such a carrier can be easily generated by spreading the reference symbol for κ times. We modulate the tag data onto the modulatable part and use the reference symbol to demodulate the tag data by the single commodity radio. κ is the spread factor for data transmission, and the proportion of productive and tag data can be flexibly controlled by changing κ. Note that our modulation is all in the payload field, which does not affect the parameter information of the signal ensuring the acquisition of the signal.

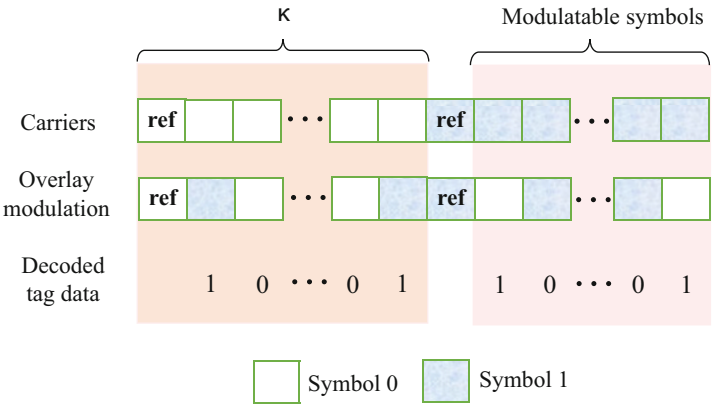


Fig. 9.10 Overlay modulation

The tag adopts codeword translation from Hitchhike [28] and FreeRider [29] to do reference-based overlay modulation upon receiving productive carriers. Due to the different characteristics of the four protocols, the method of tag modulation differs from each other. Some of them use phase modulation and some use frequency modulation. Therefore, we will discuss the tag-modulation and demodulation in detail for Wi-Fi (802.11b and 802.11n), Bluetooth, and ZigBee as follows.

802.11b 802.11b excitation signals support DSSS-BPSK, DSSS-DQPSK, and CCK modulation. We modulate tag data by BPSK that is compatible with all the above modes. When the tag bit is '1', we phase shift an 802.11b symbol for π, and when the tag bit is '0', we do nothing and keep the phase unchanged. For tag data demodulation, we just need to perform a simple XOR operation of the original data and backscatter data. In an ideal scenario, a single tag bit can be easily modulated onto one 802.11b symbol. However, the decoding performance is unstable due to signal interference and modulation errors. Taking inspiration from Miller code used in RFID systems, which employs longer modulation lengths to overcome low SNR, we introduce a spreading factor γ to increase the number of symbols used to modulate a tag data. For instance, when $\gamma = 8$, a reference symbol takes $8\,\mu s$ for 1 Mbps 802.11b, which means that we use 8 symbols to embed one tag data.

802.11n Although both 802.11b and 802.11n are Wi-Fi protocols, 802.11n is much more complicated as it uses OFDM mode, which is also involved in 802.11g/a/ac. For 802.11n, the modulation scheme includes OFDM-BPSK, OFDM-QPSK, and OFDM-QAM. We find that although OFDM has multiple orthogonal subcarriers, the BPSK modulation of the tag is still applicable because its main operation, the IFFT, is a linear operation [40]. Compared to 802.11b, the unit of tag-data modulation changes to an OFDM symbol, with a duration of $4\,\mu s$ each. What's more, it is important to note that the scrambler and BCC encoder do not compatible with codeword translation bringing broken structures in the modulated signals. Tag-

data modulation cannot convert an OFDM symbol consisting entirely of 1 s into an OFDM symbol of all 0 s. To address this, we propose to involve majority voting for the middle half part of the modulated symbols [9].

ZigBee The modulation scheme for ZigBee adopts OQPSK (offset quadrature phase-shift keying). Although ZigBee also uses PSK modulation like Wi-Fi, the introduction of the chip concept in ZigBee makes tag modulation difficult. Specifically, each ZigBee symbol consists of 4 bits, which are mapped to a 32-chip PN code. These chips are then rearranged into an IQ series, with a constant half-chip offset in between. Such a design effectively reduces PARP (peak-to-average power ratio) but leads to worse performance for BPSK tag modulation. The half-a-chip offset structure would be damaged by a phase shift of π. An effective solution is to increase the spread factor γ. In this way, even if the first symbol can not be demodulated correctly, the subsequent symbols can still be successfully decoded. This is because commodity ZigBee radios select the best-matched sequence from a set of 16 predefined PN sequences. Experimental results show that the BER achieves as low as 0.1% when $\gamma = 3$.

Bluetooth Finally, we discuss how to modulate tag data on a Bluetooth signal. Bluetooth supports GFSK (Gaussian Frequency-Shift Keying) modulation scheme [41], which is distinctly different from the first three protocols. Therefore, instead of using the PSK-based modulation method, it employs the FSK-based one. For Bluetooth excitation signals, they use f_0 to represent symbol 0, and f_1 to represent symbol 1. There is a modulation index, defined as $\frac{f_0 - f_1}{f_m}$ for commodity BLE radios, where f_m is the modulation frequency. Generally, the index is set as 0.5. In this manner, we can know that when $f_m = 1\,\text{MHz}$, $f_0 - f_1 = 500\,\text{kHz}$. Then, we modulate the tag bit 1 by shifting a frequency of $\Delta f = 500\,\text{kHz}$ and keep the frequency unchanged when the tag bit is 0.

9.3.5 Event-Driven State Machine

The above protocol identification and overlay modulation can be effectively achieved when the power of the system is stable. However, the multiscatter prototype's peak power consumption is excessively high for a battery-free tag. Therefore, we consider further reducing the system power in the following two ways:

(1) FPGA: Although we have used the lowest power FPGA (AGLN250) on the market, it still consumes two-thirds of the total system power. What we expected is that the FPGA works at full speed only when the excitation achieving. At other times, it can sleep to reduce power consumption. Fortunately, we can leverage its "Flash*Freeze" low-power mode to realize this goal. This mode allows the FPGA core to remain static while preserving all register states.

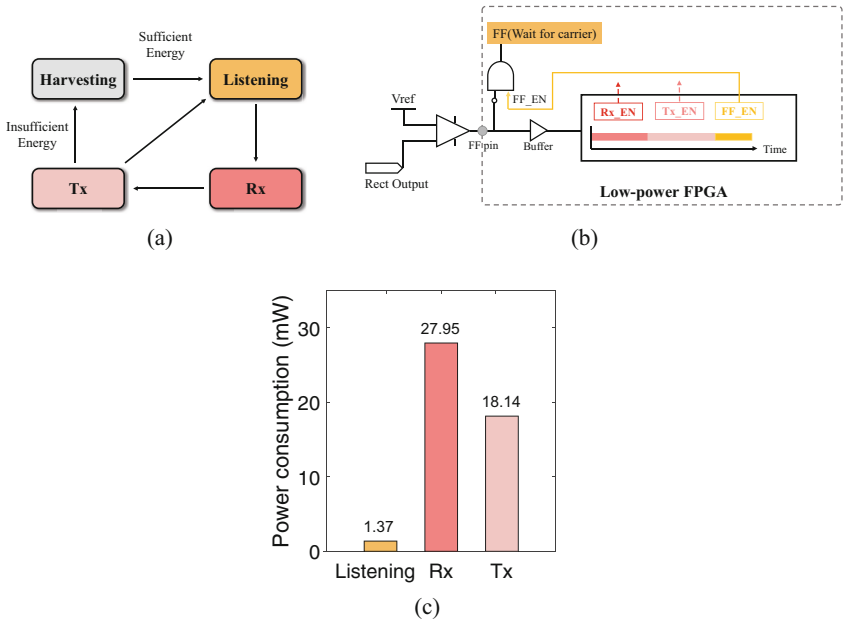


Fig. 9.11 Multiscatter low-power listening design. (**a**) Four system states. (**b**) Low-power listening control logic. (**c**) Power at different states

(2) Multiscatter prototype: In addition to setting the state of the FPGA, we devise four distinct working states for the multiscatter system as shown in Fig. 9.11. When there is no excitation, our system can work in a low-power listening mode. First, we give a detailed introduction to the four states.

- *Harvesting.* The energy harvesting module is designed to store the energy needed to operate the system. When there is no energy, the system remains in the $Harvesting$ state until an adequate amount of energy is accumulated. During this state, only the harvester component operates while all other parts of the system are shut down. Note that the system is initialized in this state every time.
- *Listening.* When enough energy has been collected, the system turns into a $Listening$ state waiting for excitation signals. Only the comparator and oscillator remain active during this mode and it consumes just 1.37 mW as shown in Fig. 9.11c. Other power-hungry operations like identification and modulation are temporarily halted.
- *Rx.* When an excitation comes, multiscatter turns into Rx state to identify the excitation protocols. During this stage, the system runs at full speed and all components are active. Figure 9.11c demonstrates that this stage has the highest power consumption, reaching 27.95 mW.

- *Tx.* The fourth stage is for data transmission. During this state, the system engages in two main activities: reading sensor data and performing overlay modulation for sensor data transmission. By bounding these two operations, we effectively minimize the active time of the system. Note that the components used for data acquiring such as the ADC, are shut down. The power consumption for this stage is about 18.14 mW.

Figure 9.11a shows the switching modes between the four states. Generally, the four states are essentially sequential, but if there is still enough energy stored when the Tx stage is completed, the system can turn to the $Listening$ stage directly. We use three enable signals, FF_{EN}, Rx_{EN}, and Tx_{EN}, to control the state switching as shown in Fig. 9.11b. The specific steps are shown below:

- *Entering and exiting Harvesting state.* When the system is initialized or the stored energy is not enough for the following operations, it enters the $Harvesting$ state and cuts off the power supply. In contrast, when a sufficient amount of energy has been harvested, $FFpin$ enables the "Flash*Freeze" control and is set to logic low. Then, the harvesting management chip restores the power supply and the systems turn into the $Listening$ state.
- *From listening to Rx.* We use a comparator to listen to the arrival of excitations. When the input data after the rectifier exceeds the threshold voltage of the comparator, We determine that a packet is coming and the $FFpin$ turns to logic high. All components in the FPGA are woken up and the system enters the Rx state. In this case, the three enable signals are set as $FF_{EN} = 0$, $Rx_{EN} = 1$, and $Tx_{EN} = 0$.
- *From Rx to Tx.* Once we finish the protocol identification, the ADC sampling and identification components are shut down and the tag enters Tx state. During this stage, $FF_{EN} = 0$, $Rx_{EN} = 0$, and $Tx_{EN} = 1$. The system will read data from sensors and do overlay modulation on the productive carriers.
- *From Tx to Listening.* When finishing the backscatter transmission, the $FFpin$ returns to logic low and the system turns to the $Listening$ state again. The enable signals are set as $FF_{EN} = 1$, $Rx_{EN} = 0$, and $Tx_{EN} = 0$.

9.4 Performance Evaluation

9.4.1 Implementation

We prototype multiscatter by a series of commodity radios and FPGA. Specifically, our system contains four main parts: a power harvesting module, a signal detector, an ultra-low-power FPGA, and an RF front-end. BQ25570, a TI harvesting chip, is used to manage the harvested energy from MP3-37, a solar panel. We used a 1000 μF capacitor to store the energy. The detector consists of a rectifier circuit and a comparator NCS2200. When the signals are coming, the output of the comparator

is high and the system is wakened up. AGLN250, a low-power FGPA, is used for all baseband processing, e.g., multiprotocol identification, and tag modulation. Finally, the control signals are output to the RF switch ADG902.

For Wi-Fi, we set the transmission rate at 1 Mbps for 802.11b and set MCS = 0 for 802.11n. Qualcomm Atheros AR938X NICs are used as transceivers for both protocols. For BLE, the transmission rate is set at 1 Mbps. A TI CC2540 and a TI CC2650 are employed as the transmitter and receiver, respectively. For ZigBee, the receiver is the same as BLE, and we use a TI CC2530 as the transmitter.

9.4.2 Evaluation

9.4.2.1 Power Consumption

Protocol-Identification Power Efficiency First, we discuss the power-saving performance of our designed protocol identification method. Several implementations, e.g., without quantization or downsampling and different sampling rate, are compared with our system in Table 9.3. Results show that the power consumption reduces from 564 mW to 12 mW thanks to our quantization process. By utilizing a 2.5 Msps sampling rate and applying quantization simultaneously, the power consumption is reduced to 2 mW, resulting in a remarkable power reduction of 282 times. Note that we simulate the power consumption on a XILINX Artix-7 FPGA here since it is complex to deploy such processes on an AGLN250.

Prototype and IC-Implementation Power Consumption We first use the FPGA to prototype our system and measure the power consumption of each component in the *Rx* state with a Keysight 34450A digital multimeter. Table 9.4 shows that the total power consumption is 27.95 mW, where the FPGA consumes 18.19 mW, the ADC consumes 7.89 mW, the oscillator consumes 0.59 mW, the RF-switch consumes 1.1 mW, and the comparator consumes 0.18 mW. The FPGA account for

Table 9.3 Required and power consumption and hardware resources for multiprotocol identification

Setup	Power(mW)	Relative ratio	LUTs
20 MS/s, no ±1 quan.	564	100%	34,751
20 MS/s, ±1 quan.	12	2.1 %	1574
2.5 MS/s, ±1 quan.	2	0.35 %	1070

Table 9.4 Power consumption of our COTS prototype

	Component power consumption					
Implemention	Digital core	ADC	Oscillator	Switch	Comparator	Total
Prototype	18.19 mW	7.89 mW	0.59 mW	1.1 mW	0.18 mW	27.95mW
IC	275 μW	237 μW	202 μW	4 μW	10 μW	728 μW
	(1.5%)	(3%)	(34%)	(0.3%)	(1.25%)	(2.6%)

most of the power consumption since it needs to generate the 30 MHz clock signal using the phase-locked loop (PLL) in addition to doing system control.

Additionally, we conduct an IC implementation simulation to optimize the system power consumption. In our simulation, we replace the power-intensive PLL with a ring-oscillator consuming about 202 μW to directly generate the 30 MHz signal. The FPGA's role is limited to realizing the digital core, with a power estimation of 275 μW using the Libero power verification tool. Since the ADC design is beyond the scope of our study, we rely on power consumption data from reference works [42]. These references indicate that an ADC operating at more than 5 Msps consumes less than 237 μW. Considering our use of a 2.5 Msps ADC, we estimate the ADC power to be around 237 μW. Eventually, the total power consumption is reduced to 728 μW, which is even much lower than low-power active radios like ZigBee.

9.4.2.2 End-to-End Performance

Next, we will measure the end-to-end transmission performance for our system.

Tradeoffs Between Productive and Tag Data From Sect. 9.3.4.1, we have known that there are two factors in overlay modulation: κ determines the number of modulatable symbols, and γ denotes the length of the reference symbol. Since the productive data and tag data are carried in the same packet, we can make a flexible tradeoff between them. Table 9.5 shows the three modes we defined to evaluate the system performance. For mode 1, the ratio of modulatable symbols and reference symbols is 1:1, and that of mode 2 is 3:1. Mode 3 carries only one reference symbol and maximizes the number of modulatable symbols pushing the ratio to an extreme. We choose proper γ for each protocol to achieve the best performance.

We test the throughput for four protocols in the above three modes and the results are demonstrated in Fig. 9.12. Overall, for the four protocols, the performance is essentially similar in the three modes. In mode 1, we observe that the throughputs for both productive and tag data are relatively the same. The maximal aggregated throughput for BLE is 278.4 kbps, with productive data throughput at 141.6 kbps and tag data throughput at 136.8 kbps. For mode 2, the throughput of tag data is about 3x that of productive data due to the 3× increase in the number of modulatable symbols compared to reference symbols. As expected, in mode 3, there is almost no productive data throughput, and tag data throughput is maximized, which is consistent with our settings. By taking advantage of the overlay modulation design,

Table 9.5 Three modes overlay modulation. Adjusting κ to tradeoff the amount of productive data and tag data

Protocol	γ	Mode 1 κ	Mode 2 κ	Mode 3 κ
802.11b	$\gamma = 4$	8	16	$4n$
802.11n	$\gamma = 2$	4	8	$2n$
BLE	$\gamma = 2$	8	16	$4n$
ZigBee	$\gamma = 2$	4	8	$2n$

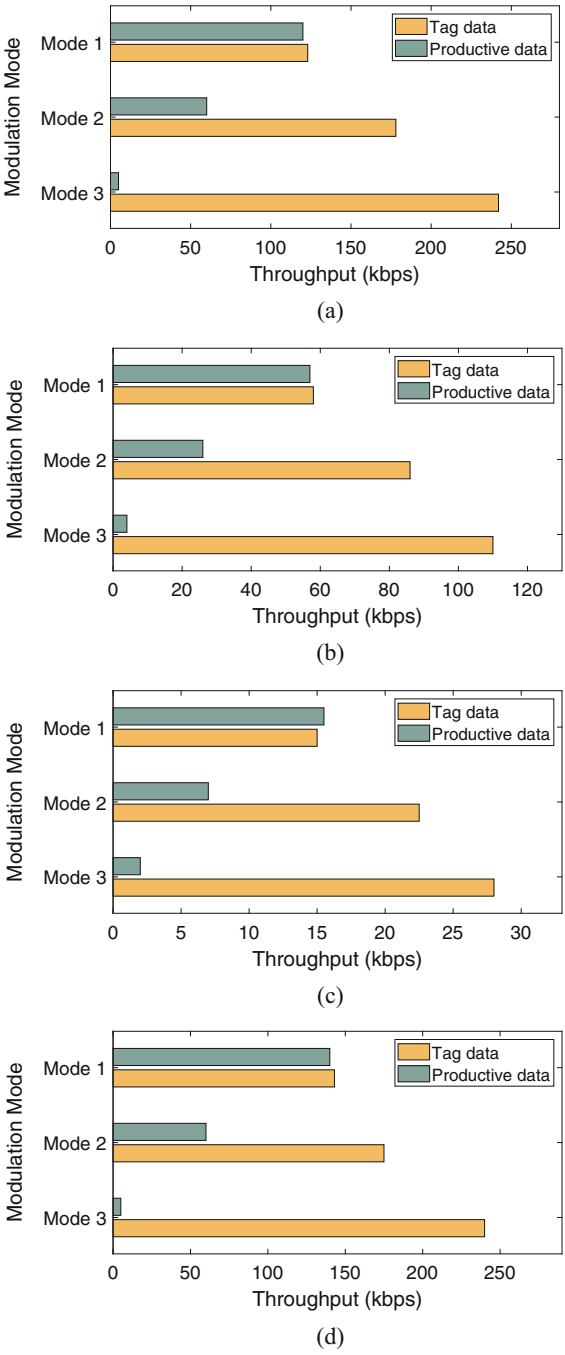


Fig. 9.12 Throughputs tradeoffs under different modes for four protocols. (**a**) Wi-Fi 802.11b. (**b**) Wi-Fi 802.11n. (**c**) ZigBee. (**d**) Bluetooth

we can make a flexible tradeoff by adjusting κ according to different application requirements. Since mode 1 provides the best balance between the two types of data, it serves as our default setting for the remaining evaluation.

Backscatter Transmission Performance Figure 9.13 shows the transmission performance for multiscatter in the LoS scenario. We fix the tag 0.8 m away from the excitations and move the receiver away from the tag from 2 m to 20 m. We mainly measure the RSSI, BER, and throughput for four protocols. Figure 9.13a shows that the RSSI decreases from −60 dBm to −85 dBm with the distance increase from 2 m to 20 m. From Fig. 9.13b, we can see that the BERs for four protocols remain low even when the tag is positioned as far as 16 m away from the receiver. Furthermore, Fig. 9.13c demonstrates the maximal aggregate throughputs achieved by multiscatter: 278.4 kbps for Bluetooth, 219.8 kbps for 802.11b, 101.2 kbps for 802.11n, and 26.2 kbps for ZigBee.

Impact of Collided Excitations To further assess the performance of multiscatter, we investigate its behavior when different excitations collide in both the time and frequency domains. As shown in Fig. 9.14a, we illustrate the collision of two excitations in the time domain. The first excitation is an 802.11n signal transmitted at 2.417 GHz, with a packet rate of 2000 pkts/s and a packet length of 300 bytes. The second excitation is a BLE signal at 2.432 GHz, with a packet rate of 34 pkts/s. Such a setup is based on the fact that Wi-Fi packets are more intense and longer than BLE packets in real scenarios. Due to the absence of filters in multiscatter, both excitations collide on the tag. Figure 9.15a indicates that the throughput for 802.11n remains relatively stable while the throughput for BLE drops rapidly from 278 kbps to 92 kbps. The difference in performance degradation is due to the higher packet rate for Wi-Fi. Therefore, to preserve BLE throughput in such collision scenarios, the implementation of filters on the tag is necessary. We will improve that in our future work. Furthermore, we measure the case where two excitations collided in frequency as shown in Fig. 9.14b. The 802.11n excitation remains unchanged, while the other excitation consists of ZigBee signals transmitted at 2.415 GHz with a rate of 20 pkts/s. Each ZigBee packet has a length of 200 bytes. Figure 9.15b illustrates that the throughputs of both ZigBee and 802.11n are not significantly affected by the frequency collisions. This can be attributed to the fact that the two excitations do not overlap in the time domain. Moreover, our ordered template matching method can effectively distinguish these packets.

9.4.2.3 Leveraging Excitation Diversity

Adaptation to Discontinuous Excitations In realistic scenarios, it is uncommon for a specific excitation signal to be present continuously and steadily. In most cases, various types of excitation signals may occur intermittently. When the system can only recognize a single signal, the system will not work when that signal is interrupted. We design an experiment to demonstrate this phenomenon. As shown in Fig. 9.16, the 802.11b and 802.11n excitation signals occur alternately. We

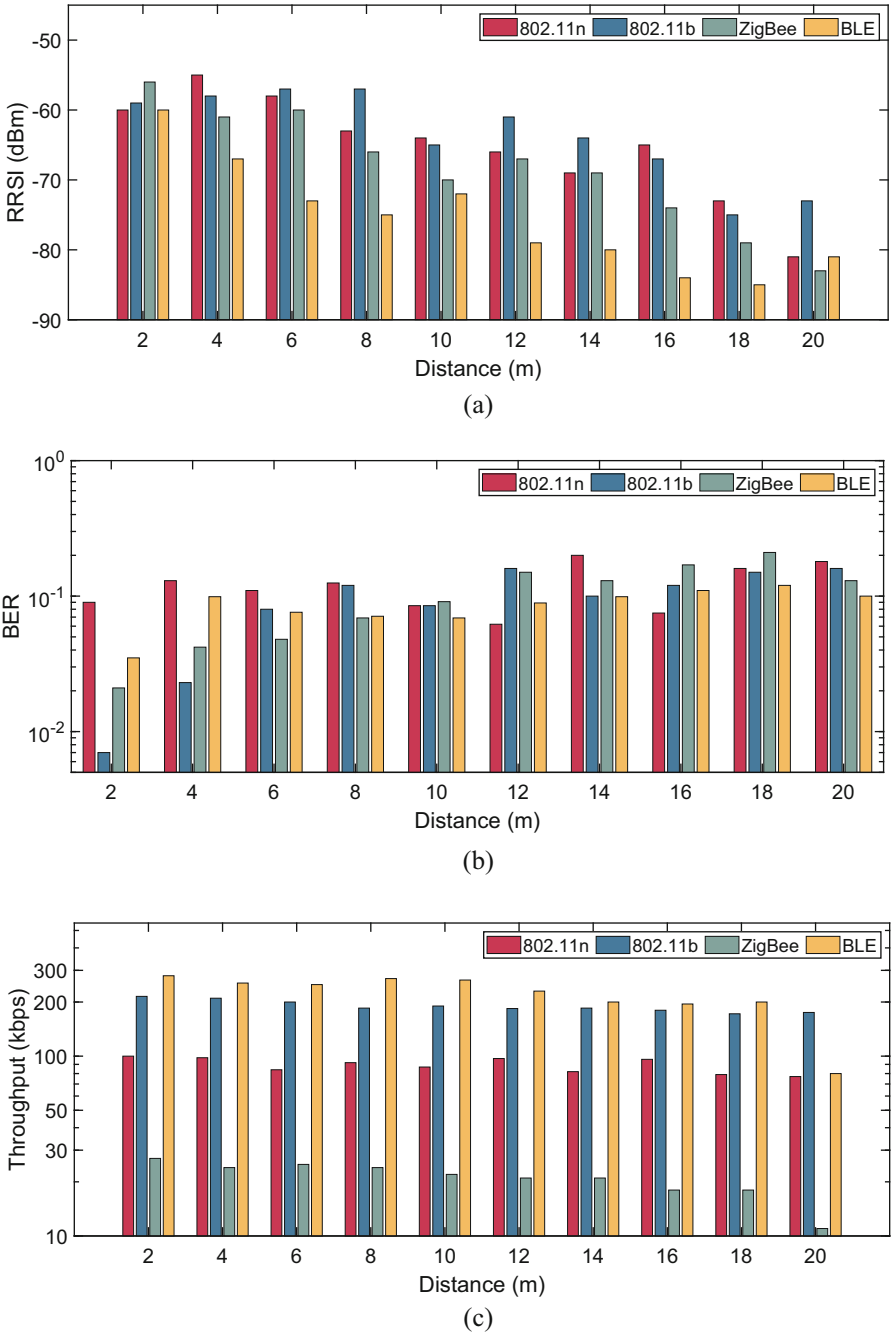


Fig. 9.13 Backscatter transmission performance across distances in LoS deployment. (**a**) RSSI. (**b**) BER. (**c**) Throughput

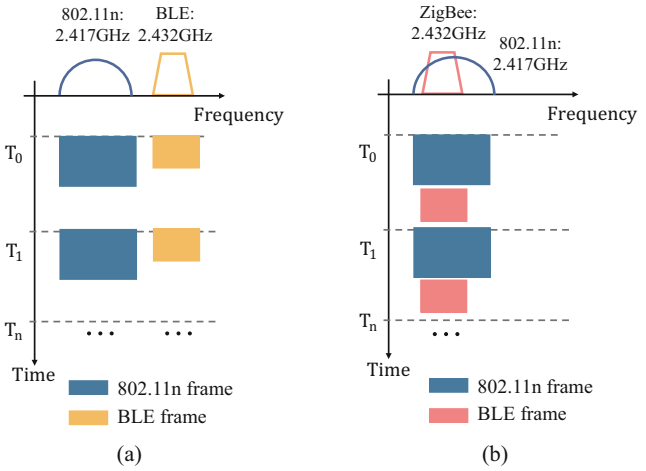


Fig. 9.14 Diverse excitation carriers collide in the time domain and frequency domain. (**a**) Excitations collide in time. (**b**) Excitations collide in frequency

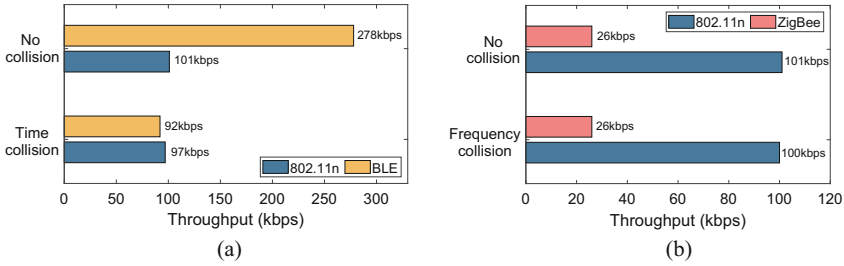
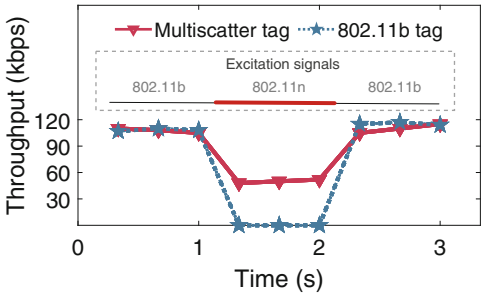


Fig. 9.15 Throughput performance when diverse excitation carriers collide in the time domain and frequency domain. (**a**) Throughput comparison of time collisions. (**b**) Throughput comparison of frequency collisions

Fig. 9.16 Throughput of uninterrupted backscatter using multiple excitations



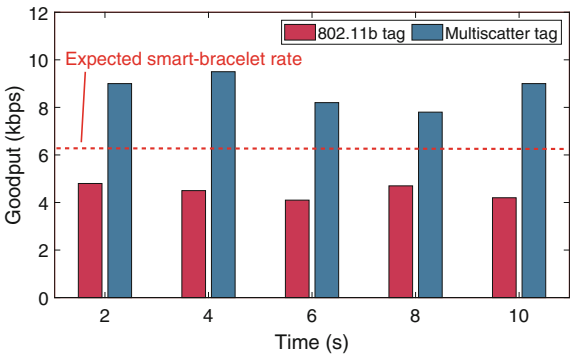


Fig. 9.17 Goodput when using intelligent carrier pick

employ our multiscatter tag and 802.11b tag in this case and measure the system throughputs. The throughput of the 802.11b tag drops to 0 when there are no 802.11b signals. In contrast, the multiscatter tag remains engaged in transmitting data continuously. Such a significant disparity arises because multiscatter has the ability to identify the different protocols and then adapt its transmission accordingly so that it can exploit excitation diversity well.

Mixed Excitation Signals There are a variety of excitation signals in the environment and the amount of each varies in different scenarios. When the system can only make use of one of these, the other resources are wasted. We test the performance of multiscatter tag and 802.11b tag in a scenario with a large number of 802.11n and a small number of 802.11b. Figure 9.17 shows that our multiscatter tag intelligently identifies that the current 802.11n excitation signal yields the highest backscattered goodput and selects it as its excitations to achieve a high goodput objective. It can meet the transmission needs of smart bracelets used for body monitoring. By comparison, 802.11b fails to work in such a scenario.

9.5 Application Case

Since the multiscatter can take advantage of the diversity of signals, the stability of the system has been greatly improved. When one excitation signal is not available, other excitation signals can be used to ensure that the data is transmitted properly. Here, we give an interesting application for multiscatter.

9.5.1 Personal Health Monitoring

In the future, the use of a large number of micro-sensors, including invasive sensors and non-invasive ones, for body monitoring will become an unstoppable trend. For

example, we can use battery-free contact lenses to monitor eye fatigue levels. The battery-free sweat sensor attached to the skin senses the composition of the sweat and analyses the condition of the body. Battery-free sensors can also be implanted under the skin to monitor blood flow to prevent cardiovascular disease. These sensors need to acquire sufficient excitation signals in order to transmit the collected data to the receiver. In the past, systems supported only one excitation signal, and when people moved to an environment where that signal was weak and other signals were strong, these devices will fail to work. However, our system supports multiple signals such as Wi-Fi, Bluetooth, ZigBee, etc. Wi-Fi and Bluetooth signals can be accessed very easily, as our mobile phones support both, and people nowadays carry their mobile phones with them almost all the time. ZigBee networks are also used in a wide range of applications including home automation, home security, industrial field control, environmental control, medical care, transportation, and more. Therefore, our system ensures the stable operation of the system and enables continuous monitoring of human health.

9.6 Summary

In this chapter, we propose, multiscatter, a new backscatter system that can efficiently identify and exploit multiple environmental excitation signals. Extensive experiments have proven the effectiveness and feasibility of the system. This capability can seamlessly integrate into existing wireless infrastructure that is extensively deployed, opening up new possibilities for IoT applications. This work significantly extends the universality of the backscatter system and takes a solid step toward large-scale deployment of the system.

In this part, we present multi-hop and multi-source backscatter systems that provide advanced solutions for the widespread use and networking of backscatter systems. Next, we will introduce two interesting applications in the following part.

References

1. Varshney A, Harms O, Pérez-Penichet C, Rohner C, Hermans F, Voigt T (2017) Lorea: A backscatter architecture that achieves a long communication range. In: Proceedings of the ACM SENSYS
2. Wang J, Hassanieh H, Katabi D, Indyk P (2012) Efficient and reliable low-power backscatter networks. In: Proceedings of the ACM SIGCOMM
3. Eletreby R, Zhang D, Kumar S, O. Yağan (2017) Empowering low-power wide area networks in urban settings. In: Proceedings of the ACM SIGCOMM. ACM, pp 309–321
4. Naderiparizi S, Hessar M, Talla V, Gollakota S, Smith JR (2018) Towards battery-free hd video streaming. In: Proceedings of the USENIX NSDI
5. Hessar M, Najafi A, Gollakota S (2019) Netscatter: Enabling large-scale backscatter networks. In: Proceedings of the USENIX NSDI

6. Vasisht D, Zhang G, Abari O, Lu H, Flanz J, Katabi D (2018) In-body backscatter communication and localization. In: Proceedings of the ACM SIGCOMM
7. Ma Y, Luo Z, Steiger C, Traverso G, Adib F (2018) Enabling deep-tissue networking for miniature medical devices. In: Proceedings of the ACM SIGCOMM
8. Jang J, Adib F (2019) Underwater backscatter networking. In: Proceedings of the ACM SIGCOMM
9. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of the ACM MobiSys
10. Ensworth JF, Reynolds MS (2017) Ble-backscatter: ultralow-power iot nodes compatible with bluetooth 4.0 low energy (ble) smartphones and tablets. IEEE Trans Microwave Theory Tech 65(9):3360–3368
11. Hu P, Zhang P, Rostami M, Ganesan D (2016) Braidio: an integrated active-passive radio for mobile devices with asymmetric energy budgets. In: Proceedings of the ACM SIGCOMM
12. Rostami M, Gummeson J, Kiaghadi A, Ganesan D (2018) Polymorphic radios: a new design paradigm for ultra-low power communication. In: Proceedings of the ACM SIGCOMM
13. Zhao J, Gong W, Liu J (2020) Towards scalable backscatter sensor mesh with decodable relay and distributed excitation. In: Proceedings of the ACM SENSYS
14. Gong W, Chen S, Liu J, Wang Z (2018) Mobirate:mobility-aware rate adaptation using phy information for backscatter networks. In: Proceedings of the IEEE INFOCOM
15. Chen S, Gong W, Zhao J, Liu J (2020) High-throughput and robust rate adaptation for backscatter networks. IEEE/ACM Trans Netw 28(5):2120–2131
16. Gong W, Liu J, Liu K, Liu Y (2016) Toward more rigorous and practical cardinality estimation for large-scale rfid systems. IEEE/ACM Trans Netw 25(3):1347–1358
17. Gong W, Liu H, Liu J, Fan X, Liu K, Ma Q, Ji X, Channel-aware rate adaptation for backscatter networks. IEEE/ACM Trans Netw 26(2):751–764
18. Gong W, Chen S, Liu J (2017) Towards higher throughput rate adaptation for backscatter networks. In: Proceedings of the IEEE ICNP
19. Wang A, Iyer V, Talla V, Smith JR, Gollakota S (2017) fm backscatter: Enabling connected cities and smart fabrics. In: Proceedings of the USENIX NSDI
20. Liu V, Parks A, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. In: Proceedings of the ACM SIGCOMM
21. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In Proceedings of the ACM SIGCOMM
22. Kellogg B, Parks A, Gollakota S, Smith JR, Wetherall D (2014) Wi-fi backscatter: Internet connectivity for rf-powered devices. In: Proceedings of the ACM SIGCOMM
23. Bharadia D, Joshi K, Kotaru M, Katti S (2015) Backfi: High throughput wifi backscatter. In Proceedings of the ACM SIGCOMM
24. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of the ACM SIGCOMM
25. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: Bringing low power to wi-fi transmissions. In: Proceedings of the USENIX NSDI
26. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) Plora: A passive long-range data network from ambient lora transmissions. In: Proceedings of the ACM SIGCOMM
27. Talla V, Hessar M, Kellogg B, Najafi A, Smith JR, Gollakota S (2017) Lora backscatter: Enabling the vision of ubiquitous connectivity. In: Proceedings of the ACM IMWUT
28. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: Practical backscatter using commodity wifi. In: Proceedings of the ACM SenSys
29. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: backscatter communication using commodity radios. In Proceedings of the ACM CONEXT
30. Zhao J, Gong W, Liu J (2018) X-tandem: towards multi-hop backscatter communication with commodity wifi. In Proceedings of the ACM MOBICOM
31. Vougioukas G, Bletsas A (2018) Switching frequency techniques for universal ambient backscatter networking. IEEE J Sel Areas Commun 37(2):464–477

32. Gong W, Yuan L, Wang Q, Zhao J (2020) Multiprotocol backscatter for personal iot sensors. In: Proceedings of the 16th international conference on emerging networking experiments and technologies, pp 261–273
33. Yuan L, Wang Q, Zhao J, Gong W (2022) Multiprotocol backscatter with commodity radios for personal iot sensors. IEEE/ACM Trans Netw
34. Lozano-Nieto A (2017) RFID design fundamentals and applications. CRC Press, Boca Raton
35. WISP 5.0. https://github.com/wisp/wisp5.
36. Zhang X, Shin KG (2011) E-mili: energy-minimizing idle listening in wireless networks. In: Proceedings of the ACM MOBICOM
37. Lu F, Ling P, Voelker GM, Snoeren AC (2014) Enfold: downclocking ofdm in wifi. In: Proceedings of the ACM MOBICOM
38. Lu F, Voelker GM, Snoeren AC (2013) Slomo: Downclocking wifi communication. In: Proceedings of the USENIX NSDI
39. Tse D, Viswanath P (2005) Fundamentals of wireless communication. Cambridge University Press, Cambridge
40. Smith SW, et al (1997) The scientist and engineer's guide to digital signal processing. California Technical Publishing, San Diego
41. ZigBee. https://zigbee.org/zigbee-for-developers/zigbee-3-0/
42. Wan K, Hong H, Roh Y, Kang H, Hwang S, Jo D, Chang D, Seo M, Ryu S (2016) A 0.6 v 12 b 10 ms/s low-noise asynchronous sar-assisted time-interleaved sar (sati-sar) adc. IEEE J Solid-State Circuits 51(8):1826–1839

Part IV
Innovative Backscatter-Enabled Applications

On top of reliable communication and networks, part IV proposes two novel applications that are thought impossible before, lightweight spatial sound recording over the air (Chap. 10) and self-powered wireless wearables for healthcare (Chap. 11).

Chapter 10
Microphone Array Backscatter

Abstract It has been demonstrated that backscatter enables ultra-low-power and ubiquitous wireless connectivity. Benefiting from the simple structure and passively reflecting mode, backscatter can also be technically customized to fit specific application scenarios. Traditional microphone array designs are faced with a significant challenge of precise synchronization. They use complex digital processing for this, causing the need for bulky and power-consuming hardware. In this chapter, we just showcase its superiority when used in multi-track audio streaming. Specifically, a novel microphone array sensor architecture that enables synchronous concurrent transmission of multi-track audio signals using analog backscatter communication is introduced. The key enablers are Pulse Position Modulation (PPM) and Differential Pulse Position Modulation (DPPM) baseband circuits that can generate a spectral-efficient, time-multiplexing, and multi-track-synchronous baseband signal for backscattering. Around those two novel designs, we also provide hardware and software customizations to realize low-power and high-quality spatial sound recording. In this way, power-hungry RF transceivers, DSPs, and codecs can be avoided and the spatial audio quality can be satisfied. A microphone array prototype based on low-power FPGA has been developed to show its effectiveness. Experimental results show that our design supports a communication range of 28 m, and as many as 8 audio tracks can be realized. The corresponding throughput reaches 6.4 Mbps when the audio sampling rate is 48 kHz. The latency with 4 audio tracks is only 87.4 μs, corresponding to 650× improvement over digital designs. The whole power is estimated to be 175.2 μW in ASIC design, which is affordable by harvesting RF or sound energy. Finally, three applications based on our microphone array backscatter design are introduced: an acoustic imaging system, a beamforming filter, and a voice control system.

10.1 Introduction

Acoustic sensing and communication technologies have drawn the attention of both academic and industry [1–10]. The spatial sound technology is especially popular as it contributes to 3D sound in AR/VR and acoustic cameras. There are already some

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_10

multimedia platforms supporting spatial sound. For example, Apple Music in iOS devices starts to provide spatial audio service [11].

To generate spatial audio, the sound wave information from multiple directions should be gathered separately. More tracks usually lead to finer spatial resolution. And the synchronization between audio tracks is also essential in the reconstruction of spatial sound. Only when the tracks are aligned well in time domain will the subtle difference between audio tracks be extracted successfully to drive the source position or strength distribution [5, 12, 13]. In a typical deployment, the microphone array is used to simultaneously record multi-track audio signals from different directions. Many works focus on the audio-track synchronization in microphone array, but they are still unable to fit the small form factor and low power requirements in consumer wearable devices.

Digital Synchronization The newest COTS microphone array products [14, 15] usually only work to acquire sound signal. The synchronization task is transferred to the computers they are connected with. As shown in Fig. 10.1a, the synchronization between audio tracks is realized totally in the digital domain: the synchronization algorithms run on DSP or even dedicated single-board computer [16, 17]. The corresponding computational overhead and latency are very large. Still, complex components such as ADC, DSP, and codec are needed, causing unaffordable power consumption and hardware complexity in consumer devices.

Wireless Synchronization Spatial sound synchronization tasks can also be delivered to the server wirelessly. But the corresponding designs are even more complicated and heavy weighted. For example, [5] builds a microphone array using multiple smartphones and then streams recorded audio signals to the server using Wi-Fi/Cellular NIC. The synchronization and processing are realized in the server. GPS signal can also be used for synchronization of large-scale spatial audio recording [13]. In those systems, the uncertainty caused by wireless streaming renders the synchronization of audio tracks an even more complicated task.

Many factors including spatial audio quality, latency, power consumption, wireless spectral efficiency, and digital processing burden should be considered when designing wireless multi-track audio synchronization. Backscatter technology provides low-power connectivity for wireless sensors and should be a good candidate for spatial audio transmission [18–45]. But before that, we are faced with the following challenges:

1. **Protocol-oriented backscatter.** Existing backscatter systems mostly focus on using ambient wireless signals and commercial radios to ease large-scale deployment [19–25, 28, 29, 32–35, 37, 38]. They all contribute little to reducing the complexity of spatial audio acquisition and synchronization. How to replace power-hungry components including ADC, DSP, codec with light-weight ones still remains a problem.
2. **Tradeoff between complex application and light-weight analog modules.** The needed transmission rate for uncompressed spatial audio equals to the product of the sampling rate, the track count, and the sampling depth. To satisfy

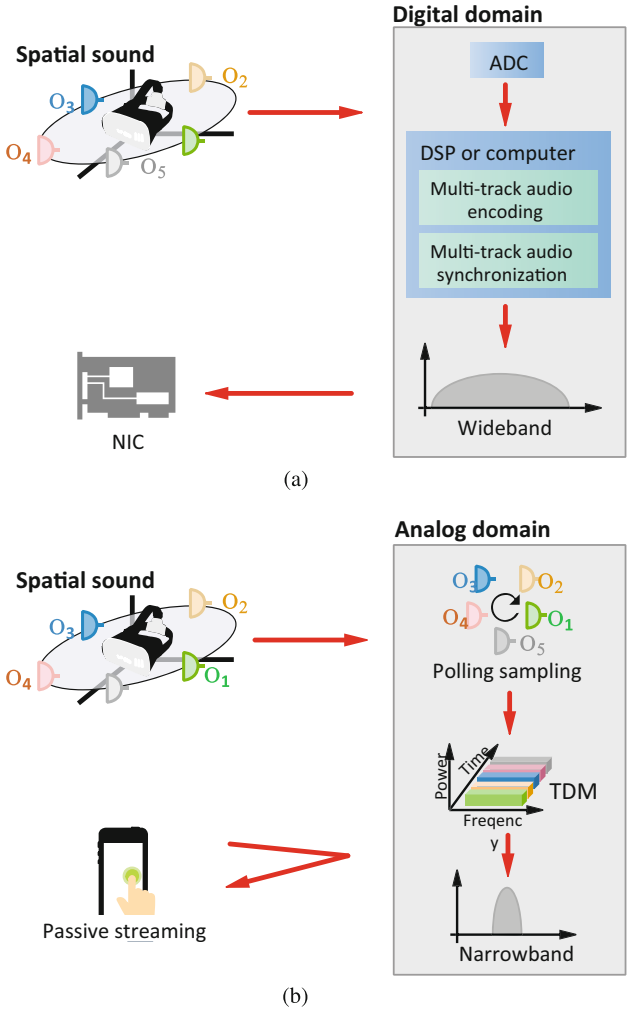


Fig. 10.1 Comparison of spatial sound streaming solutions: (a) traditional method requires heavy processing and causes high power consumption; (b) our design uses analog roll polling method and backscattering technique to sample synchronous spatial audio signal and then transmit it in one narrowband stream. (**a**) Backscatter decoding process. (**b**) $\mathcal{T}$ and $\mathcal{C}$ are not commutative

the CD audio quality, the sampling depth should be 16 bits. That leads to a throughput requirement as high as 6.14 Mbps with 8 audio tracks and 48 kHz sampling rate, as shown in Table 10.1. Existing analog backscatter systems for audio/video communication [34, 40, 45] all cannot support multi-track audio with CD quality. Their corresponding throughputs are not high enough, either. Even worse, they have no way to realize the synchronization between audio tracks.

Table 10.1 The throughput requirements for different audio settings. Data rate=sampling rate × track count × sampling depth (16 bits for CD)

	Bit rate for different sampling rates		
Track count	22.05 kHz	44.1 kHz	48 kHz
2	0.71 Mbps	1.41 Mbps	1.54 Mbps
4	1.41 Mbps	2.82 Mbps	3.07 Mbps
8	2.82 Mbps	5.64 Mbps	6.14 Mbps

3. **Power consumption.** As illustrated in Table 10.1, the throughput requirement is as high as 6.14 Mbps. This may cause high power consumption in backscatter.

For the challenges introduced above, we design a novel microphone array backscatter that is able to record synchronous multiple audio tracks and transmit them using analog backscatter technology. It is the first backscatter system to realize synchronization of multiple audio tracks with light-weight and low-power system design. The design overview can be seen in Fig. 10.1b. The key idea is taking turns to record and transmitting audio signals from multiple microphones in a fixed order. Then on the receiver side, the roll polling order can be recovered and audio-track synchronization can be realized. The design is detailed as follows:

- **Customized PPM and DPPM.** We design pulse position modulation (PPM) and differential PPM (DPPM) to convert audio signals into real-time pulse positions. And to enable multiple-track audio recording, the system takes time-division multiplexing access that uses the roll polling method to check microphones one by one. And every modulated audio track takes one separate piece of time.
- **Passive transmission.** We use backscatter technology to stream audio information. The PPM or DPPM signal for every track is modulated into the RF carrier using PSK modulation immediately after it is recorded. Besides, the necessary information about the sampling rate for sound recording on every track is also embedded.
- **Low power design.** We reduce system power consumption by significantly eliminating digital synchronization and processing tasks and replacing traditional RF transceivers with ultra-low-power backscatter modules. The ASIC simulation shows that our design is able to realize a high power efficiency and fit many wearable devices.

We have also built a system prototype to show the effectiveness of our ultra-low-power synchronous spatial audio recording design. Experimental results show that our microphone array backscatter supports a communication range of up to 28 m with 8 audio tracks and 48 kHz sampling rate. The corresponding throughput reaches 6.4 Mbps. And the latency with 4 audio tracks is tested to be about 87.4 μs, which is about 650× lower than digital solutions using sound cards, dedicated coding and streaming software, and Wi-Fi/Bluetooth adapter. ASIC simulation power consumption can be optimized to about 175.2 μW with 8-track 48 kHz audio signals. Still, we showcase three applications in our microphone array backscatter prototype: an acoustic imaging system, a beamforming filter, and a voice control system. They all prove the effectiveness and superiority of our design. Finally, there

are some limitations on our design, which can be summarized as follows. (1) System has a limited communication range. That's because we use an RC integrator for decoding analog data, and when the signal is weak the fidelity will be seriously influenced. (2) In the PPM design, a synchronization clock is needed for each sampling cycle and may cause additional power consumption; (3) A specialized reader is needed to generate single-tone excitation and demodulate the backscatter signal, which may cause additional deployment cost.

The main contribution of this paper is summarized as follows:

- Our design and real-world experiments prove that it is possible to use simple analog design to realize complex digital sensing data processing (e.g., the spatial audio recording and synchronization in this chapter). Further, the co-design of sensing part and backscatter transmission significantly reduces system complexity. This provides a new idea about how to bring the superiority of backscatter into full play.
- We provide a novel microphone array backscatter design that realizes spatial audio streaming with negligible latency and system power consumption. That is potential to enable multiple-track 3D audio in wearables.

10.2 Related Work

Acoustic Wearable and Sensing Systems Acoustic technologies have been developed for wearables and sensing applications in both consumer and industrial scenarios [1–10]. LipRead [1] focuses on ultrasound attack and defense. A microphone-array-based beamforming adaptive system with synchronization algorithms has also been developed [5]. Acoustic motion tracking systems with enough precision for the new interference of VR/AR applications are also very attractive [8]. [8] reuses the smartphone microphone to synthesize an array by moving it at different spatial locations and collecting reflected sound signals separately. Those works all focus on the design of digital processing algorithms. While Microphone array backscatter [46], focuses on using simple analog design to replace complex digital processing and using backscatter technology to make wireless transmission more efficient.

Protocol-Oriented Backscatter and Analog Backscatter Making backscatter compatible with commodity signals and using ambient radios as exciter or receiver has been a hot topic [19–25, 28, 29, 32–35, 37, 38, 47, 48]. But the data acquisition has not been investigated. Those protocol-oriented backscatter systems have to rely on traditional methods for spatial audio acquisition and digital synchronization. On the contrary, our microphone array backscatter system includes both the backscatter streaming module and the acoustic acquisition module that can gather synchronous audio tracks with ultra-low power. The hybrid backscatter [45] uses continuously changing RF impedance of the antenna for sensing and then streams the data using analog backscatter. Combining two aspects, a battery-free wireless microphone is

built. Our microphone array backscatter has two fundamental differences from it: (1) our design focuses on the synchronization of multiple audio tracks while the hybrid backscatter targets sensing and transmitting single-track audio using analog methods; (2) the PPM and DPPM techniques are different from its analog audio sensing technique. Battery-free cellphone [34] realizes realize bi-directional audio transmission using analog decoding and analog backscattering. But its design goal and audio acquisition circuit are different from those in our system. It targets single-track audio streaming, but we aim to realize synchronization between audio tracks. It uses the variation of JFET impedance to gather voice information, while we design PPM and DPPM to get multi-track audio. Passive video transmission is also investigated [40]. It has one single track and no synchronization should be considered. Still, the pulse width modulation instead of PPM/DPPM is used in this system.

10.3 Microphone Array Backscatter Design

We integrate spatial audio acquisition, synchronization and processing, and light-weight wireless transmission in a system to build our microphone array backscatter. To avoid power-hungry digital synchronization and processing, a specialized analog circuit is designed. The system overview is depicted in Fig. 10.2. In this section, we first introduce the analog PPM and DPPM audio modulation with synchronization and then illustrate how modulated information is streamed using backscatter technology and how the spatial audio is recovered in the receiver. Finally, we will give a whole picture of the system and provide some design thinkings.

10.3.1 Audio Modulation

Transmission of digital samples from multi-track audio needs a high data rate, which will cause high power consumption. On the other hand, the compression algorithm is unaffordable in the tag, either. Our microphone array backscatter reduces system complexity and power consumption by conducting analog sensing and streaming instead of digital processing. To keep the necessary information for spatial sound

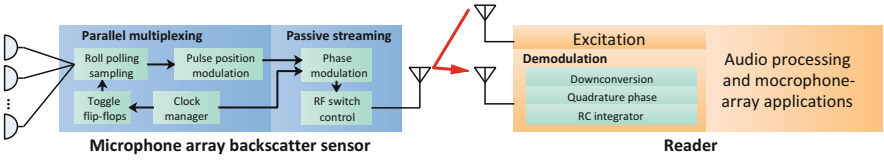


Fig. 10.2 System overview

recovery, we design PPM and DPPM solutions to sample and stream synchronous audio tracks concurrently.

10.3.1.1 Pulse Position Modulation

We do not create parallel track transmissions using frequency diversity for the difficulty in synchronization between them. Instead, we arrange different tracks in time order. They are sampled and streamed one by one on a single channel so that they are synchronous in nature.

We use the multiplex solution in controlling model aircrafts. The flying parameters including height, direction, and speed of aircrafts needed to be conveyed wirelessly. The controller encodes corresponding commands into one analog stream using PPM method and then transmits it in one wireless channel. In PPM modulation, the analog information is embedded in a narrow pulse position relative to the start of a sampling period or to the previous pulse position [49, 50].

We customized a PPM modulation scheme to realize synchronous transmission of spatial audio tracks. As shown in Fig. 10.3. The PPM circuit first uses an analog multiplexer to access a single sound channel, and then sample the corresponding audio track by comparing the sound signal with a periodic triangular wave. The comparator will output a pulse whose width stands for the voice amplitude of the current channel.

Then the pulse-width modulated sound sample will be converted into the pulse position information using an inverter and a monostable multivibrator: the falling edge of the comparator will cause an immediate narrow period in the PPM output at the monostable multivibrator. Note that the monostable multivibrator has been well studied and we can deploy a simplified version in our backscatter to reduce circuit complexity and power consumption. We will introduce it in Sect. 10.3.4. The

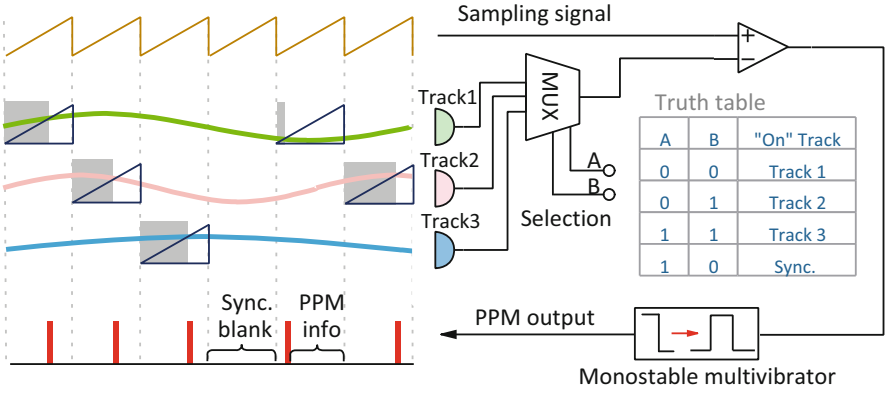


Fig. 10.3 Roll polling multiplexing design that combines synchronous PPM analog samples of multiple audio tracks to generate one stream

pulse position is relative to the start of the current sampling period. The pulse width is determined by the parameter of the monostable multivibrator and contains no information about sound waves.

We use roll polling methods to multiplex multiple audio tracks. The roll polling procedure is controlled by a synchronization clock. As shown in Fig. 10.3, two control signals generated from the synchronization clock together with a truth table are used to select the audio channel. The triangle wave which works as a sampling signal also comes from the synchronization clock. Thus, the audio-track synchronization can be satisfied.

As illustrated above, every track takes a sampling period exclusively in a polling cycle. We set the first sampling period blank without generating a sampling pulse as the synchronization period. The following periods are taken by audio tracks. Let the track number be N, and the sound sampling rate be f_a, the synchronization clock frequency be f_{syn}. Then we get the following relation.

$$f_{syn} = f_a \times (N + 1) \tag{10.1}$$

For example, in FM radio broadcasting, the sound sampling rate f_a is 22.05 kHz, then the synchronization clock f_{syn} increases from 66.15 kHz to 198.45 kHz when the audio track number increase from 8. The general CD and MP3 audio formats have a sampling rate of 44.1 kHz. The needed f_{syn} for 8 audio tracks reaches 396.9 kHz. The high-definition audio sampling rate is about 48 kHz. The corresponding synchronization clock is about 432 kHz.

10.3.1.2 Differential Pulse Position Modulation

As introduced above, the synchronization clock is needed to generate the sound channel selection control signal and decides the start of every sampling period. The receiver needs to first recover the synchronization signal then the sound information decoding can be realized. This brings additional computation burden and risk of errors. So we design DPPM, which needs no synchronization control. It cascades audio tracks and uses the feedback for multiplexing. Specifically, every track output is connected to the next track as the trigger for sampling the sound in the corresponding channel. The interval between the current pulse with that for the last channel represents the sampled sound. And the feedback from the last channel to the first one starts the next roll polling cycle.

The DPPM circuit with 3 audio tracks is shown in Fig. 10.4. It is made up of comparators, monostable multivibrators, RC calculation circuits, and an OR gate. For every audio track, we have two monostable multivibrators. The output monostable multivibrator has a narrow pulse width for ease of the end position marking. The OR gate collects outputs of every track's output monostable multivibrator to synthesize DPPM output logic. The sampling monostable multivibrator output has a wide pulse, which can be converted to a wave similar to a triangle pulse by the RC calculation circuit to start the sampling of the next sound channel and work as

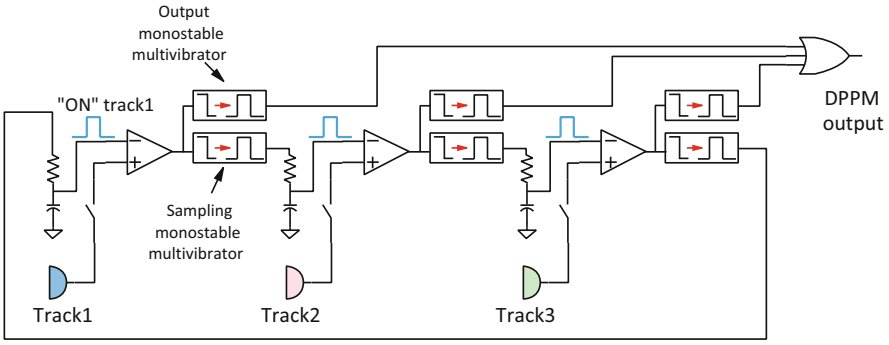


Fig. 10.4 Roll polling multiplexing design for DPPM technique that uses intervals between pulses for corresponding audio tracks to present analog sound samples

the sampling signal. The corresponding audio track will also be switched on by this wide pulse. The sampling time t_s should not be longer than the sampling monostable multivibrator output pulse width T_{smm}: $t_s \leq T_{smm}$.

T_{smm} can be set by adjusting the discrete component parameters in the monostable multivibrator. It determines the sound sampling rate. Let N be the audio track number, then the needed sound sampling rate f_a for one track should satisfy the following equation:

$$f_a \leq \frac{1}{N \times T_{smm}} \tag{10.2}$$

Then, it can be seen that $T_{smm} \leq \frac{1}{N f_a}$. When we sample 8 track FM radio whose sampling rate is 22.05 kHz, $T_{smm} \leq 5.67\,\mu$s.For the 8-track audio of CD format or DVD, T_{smm} should be less than 2.83 μs and 2.60 μs, respectively.

DPPM and PPM have distinct advantages and disadvantages that make them suitable for different applications. PPM, for instance, allows for precise control over the sampling rate. Using Eq. (10.1) and given the synchronization signal frequency f_{syn} and N tracks, PPM sets each track's sample rate at $f_{syn}/(N+1)$. PPM also provides accurate synchronization for every roll polling cycle, thanks to its synchronization blanks. On the other hand, DPPM doesn't require synchronization signals from both the sensor and reader sides, but it lacks precise control over each track's sample rate.

10.3.2 Backscatter Transmission

PPM and DPPM modulate spatial sound into one analog data stream. We investigate how to transmit it with a low-power and low-complexity system.

Let $f_s = 10\,\text{MHz}$ and $\omega_s = 2\pi\omega f_s$ be the shifting frequency and the corresponding angular frequency, respectively. Backscatter toggles the switch for different reflection states and manipulates them for frequency shifting and modulation [24, 25]. In our system, the two states are $+1$ and -1 respectively. The two distinct reflection coefficients are used to generate a square wave which can be expressed as: $M(t) = \sum_{n=1}^{\infty} \frac{sin(2n-1)\omega_s t}{2n-1}$. We modulate $M(t)$ using a time-variant phase $\phi(t)$ that contains the analog spatial sound stream to get the baseband signal $S(t)$. $\phi(t)$ can be expressed as the following equation.

$$\phi(t) = \frac{\pi}{2} + (i-1)\pi, \quad (t_i < t < t_{i+1}) \tag{10.3}$$

Where t_i represents the ith pulse position. That means the backscatter modulation phase changes for π at every pulse position. And the signal $S(t)$ to directly control the toggling of switch can be expressed as the following equation.

$$S(t) = \frac{4}{\pi} \sum_{n=1}^{\infty} \frac{2n-1}{sin((2n-1)\omega_s t + \phi(t))} \tag{10.4}$$

By feeding $S(t)$, the reflected RF signal will be shifted to another wireless channel and modulated by the analog audio samples. Figure 10.5 shows the time-domain waveform and frequency-domain spectrum. Two significant lobes can be observed in Fig. 10.5b, one for excitation signal and the other for backscattered signal. The frequency shift divides them to avoid self-interference. Still, the backscatter modulation can be seen in the backscatter spectrum lobe.

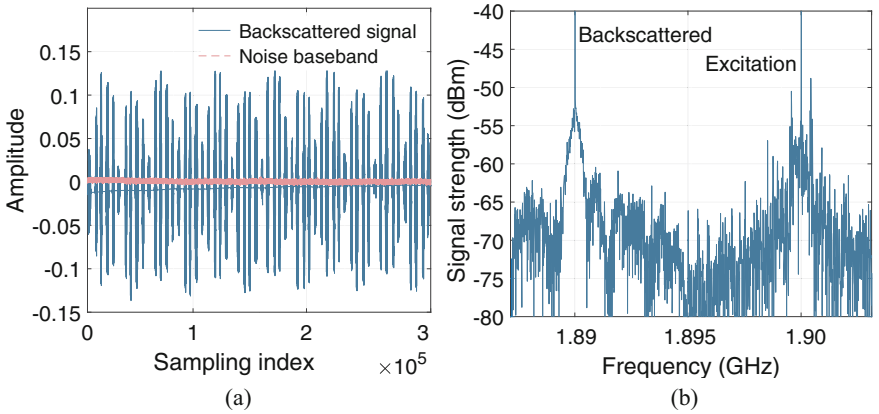


Fig. 10.5 The waveform and frequency spectrum of backscattered signal. (**a**) Time domain. (**b**) Frequency domain

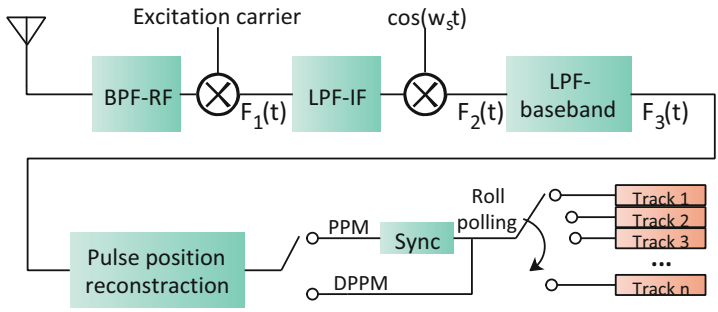


Fig. 10.6 Demodulation operations

10.3.3 Audio Regeneration

As described in Sects. 10.3.1 and 10.3.2, the microphone array backscatter follows a three-step process to transmit multi-track audio signals. Firstly, it generates a time-multiplexing baseband using either PPM or DPPM techniques. Next, it modulates this baseband on a 10 MHz frequency shift signal that changes the antenna impedance. Finally, it uses RF reflection to transmit the modulated baseband. The reader must follow three corresponding steps to demodulate each track's signal, as shown in Fig. 10.6.

The first step is extracting the baseband of backscattered signal. The backscatter modulation can be seen as a linear operation, so the coherent demodulation is used in our receiver. As shown in Fig. 10.6, the downconversion is first conducted on the bandpass-filtered signal by multiplying it with an identical copy of excitation carrier and then using a low-pass filter to remove the high-frequency component and reserve the baseband. The cutoff frequency of the low-pass filter is set larger than the shifting frequency that is 10 MHz. The result can be expressed as follows.

$$F_1(t) = A + sin(w_s t + \phi(t)) + n(t) \tag{10.5}$$

where A, n(t) stand for the amplitude of the received excitation signal and the noise.

The next step obtaining the PPM or DPPM baseband signal $\phi(t)$ from $F_1(t)$ in Eq. (10.5). The solution is still coherent demodulation. Specifically, a mixer is used to coherently multiply $F_1(t)$ with $cos(w_s(t))$, a 10 MHz signal with a $\frac{\pi}{2}$ phase difference, and then a low pass filter with cutoff frequency less than 10 MHz is used to extract the PPM or DPPM baseband. That is:

$$\begin{aligned} F_2(t) &= F_1(t)cos(w_s(t)) \\ &= Acos(w_s(t)) + sin(w_s(t) + \phi(t))cos(w_s(t)) + n_1(t) \\ &= Acos(w_s(t)) + \frac{sin(2w_s(t) + \phi(t))}{2} + \frac{sin(\phi(t))}{2} + n_1(t) \end{aligned} \tag{10.6}$$

where $n_1(t)$ is the noise after mixing. A low-pass filter with cutoff frequency lower than 10 MHz can be used to remove the high-frequency and only reserve the target signal, which can be seen in the following equation.

$$F_3(t) = \frac{sin(\phi(t))}{2} + n_2(t) \tag{10.7}$$

Where the $n_2(t)$ is the noise after low-pass filter. With good SNR it can be ignored. Then the $F_3(t)$ function has two distinct values: -1 and $+1$. Note that $\phi(t)$ only changes at the pulse positions t_i. So that by observing the transition edge of $F_3(t)$, the pulse position information can be extracted. We can recover PPM or DPPM baseband by taking all positive and negative edges of $F_3(t)$.

After obtaining the PPM or DPPM baseband, the last step is to demodulate the audio tracks. The pulses in a PPM or DPPM signal are assigned to multiple tracks based on the roll polling order. In the case of a PPM signal, a synchronization signal is required to locate the starting position of each sampling period. Finally, the decoded audio samples are assigned to corresponding audio tracks and then used to recover the spatial sound.

10.3.4 Hardware Customization

We customize the analog and digital circuits to fit the low-power PPM and DPPM modulation together with backscatter reflection.

10.3.4.1 Analog Modulation Circuits

The corresponding analog circuits for PPM and DPPM are shown in Figs. 10.3 and 10.4 respectively. We will introduce the key components including the monostable multivibrator and multiplexing & sampling circuit.

Monostable Multivibrator Our system requires the monostable multivibrator component. It can convert pulse width modulated signal to pulse position modulated one. In the analog modulation circuits, we use one monostable multivibrator for the PPM baseband and multiple ones for the DPPM baseband. Traditional monostable multivibrators involve complex circuits and thus are power-hungry. However, we have simplified the implementation with two options shown in Fig. 10.7. In Implementation I, a NAND gate together with resistors and capacitors are used to generate a narrow pulse immediately after a negative edge of the input pulse. Implementation II is even simpler. It is made up of an inverter, a diode, and an RC differential circuit. This implementation does not generate a rectangular pulse but outputs a positive edge when there is a pulse negative edge. We can use these pulse

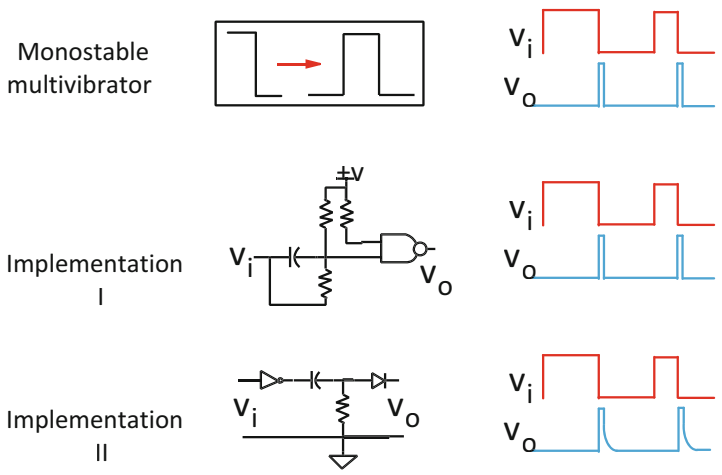


Fig. 10.7 Simplified monostable multivibrator designs

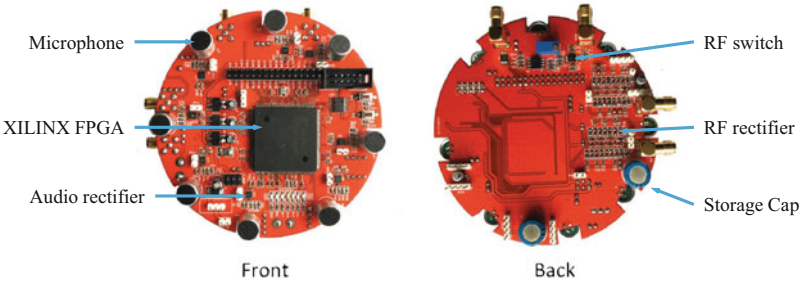


Fig. 10.8 PCB prototype of microphone array backscatter

edges to modulate data for both PPM and DPPM. Especially, Implementation II incurs very low power and can be easily realized.

Multiplexing and Sampling In our system, we use a CMOS analog multiplexer CD4051 to multiplex multi-track analog signals into one streaming channel. The CD4051 is controlled by the roll polling logic implemented in the FPGA. To sample the audio signals, we employ an RC integral circuit and a high-speed voltage comparator TLV3501. The PCB prototype is shown in Fig. 10.8.

10.4 Evaluation

We first build a microphone array backscatter using commercial components and realize the function of reader in an USRP platform. In the PCB tag prototype, 8 commercial microphones are placed evenly in a circle to support as many as 8 audio

tracks for spatial sound. Additionally, we test the power consumption of the PCB tag prototype. We also simulate the ASIC design that can realize similar functions to optimize the power consumption of our design using an ASIC design platform

We also conduct experiments to evaluate the performance of our microphone array backscatter design. We evaluate the quality of the demodulated spatial sound, including the spatial sound latency and fidelity. Still, the system performance at different exciter-to-tag and different tag-to-reader distances are tested to estimate the spatial coverage ability.

10.4.1 Implementation

In this section, we provide a detailed description of the PCB implementation of our microphone array backscatter. It is made up of an FPGA, analog devices, and discrete components. Additionally, we outline the implementation details for our reader and energy harvester, and discuss our efforts to further optimize power consumption through the use of Application Specific Integrated Circuit (ASIC) design technology. Finally, we analyze the power consumption to show system usability.

10.4.1.1 PCB Prototype

PCB Prototype As introduced above, the controller in microphone array backscatter tag is the XILINX Spartan XC3S500E-4PQ208 FPGA. It contains the logic for roll polling controlling and backscatter modulation. To control roll polling of audio tracks, the FPGA needs to produce the synchronization clock, and then use it to generate the multiplexing track selection signal. For 4-track audio multiplexing, two selection signals can be used to locate a target channel according to the truth table, as shown in Fig. 10.3. For more audio tracks, more selection signals and more complex truth table. But the computation complexity is affordable in the FPGA. The need analog components includes microphones, a CD4015 multiplexer, monostable multivibrators made up of diodes and invertors, and TLV3501 comparators for spatial audio sampling, and an ADG902 RF switch for backscatter reflection. The AND, NAND, OR, and XOR logic gates used in the audio sampling multiplexing and RF switch controlling are all realized in the FPGA.

Reader We realize the sound demodulation and recovery procedure introduced in Sect. 10.3.3 on a USRP N210 software-defined radio. A 6.5 dBic MTI MT-242025/TRH/A antenna is used as the transmission antenna. The RF excitation source is another USRP N210 device that can generate 895 MHz sinewave. To boost the excitation signal, we use an HA901I-APC RF amplifier and an 8.5 dBic RFMAX S9028PCR antenna.

10.4.1.2 ASIC Design

ASIC (Application-Specific Integrated Circuit) design can transform a customized large-scale circuit into a tiny working silicon for small size, low cost, and low power consumption. The backscatter sensor prototype includes both analog and digital circuit modules, which can be optimized through ASIC design. We also provide a customized ASIC design and analyze its power consumption using the Cadence IC6.17 Virtuoso software together with a TSMC 65 nm CMOS Low Power technology library. All the analog modules in PPM and DPPM baseband circuits are included. The power to realize their functions is provided in the ASIC simulation. The digital modules are analyzed in the synthesis tool XST and power analysis tool XPower [51] in Xilinx Integrated Synthesis Environment.

10.4.1.3 Power Consumption

In this part, we analyze the system power consumption of the ASIC design. The estimated power of PPM and DPPM are shown in Table 10.2 The corresponding results are detailed as follows: the 10 MHz oscillator takes about 142.3 μW, the monostable multivibrator takes about 9.5 μW, and the analog audio sampling circuit takes about 13.4 μW. The digital control logic power consumption is estimated to be about 10 μW. Based on those results, we can get the total power consumption of the baseband circuits. In PPM implementation, the sensor tag is composed of an oscillator, a monostable multivibrator, an analog audio sampling circuit, and a digital control module. The power consumption is calculated to be about 175.2 μW. The power consumption keeps constant when the track count rises from 2 to 8 because there is only one multiplexing and sampling circuit, and only the chosen microphone channel works normally. On the other hand, the power consumption of the DPPM baseband varies with the number of audio tracks. For instance, in Fig. 10.4, the DPPM baseband for three tracks utilizes three analog sampling circuits, six monostable multivibrators, an oscillator, and a digital circuit module. Consequently, the total power consumption of all three tracks is 249.5 μW. Although the DPPM baseband circuit eliminates the synchronization clock compared to the PPM baseband, it is more complicated and consumes more power, e.g., twice as much for 8 audio tracks.

Table 10.2 Power consumption of our design

	Baseband circuits	
Track count	PPM	DPPM
2	175.2 μW	217.1 μW
4	175.2 μW	281.9 μW
6	175.2 μW	346.7 μW
8	175.2 μW	411.5 μW

The choice between PPM and DPPM depends on user's requirements. DPPM doesn't need the synchronization clock and sampling period control, and supports more audio tracks than PPM. Its corresponding decoding is also simpler since no synchronization of sampling period is needed. But it requires more power consumption. So it can be concluded that DPPM is appropriate for more audio tracks where higher power consumption can be accepted.

10.4.2 Quality of Service

10.4.2.1 Latency

We measure the system latency, which is the time for acquiring and transmitting spatial audio in microphone array backscatter. The latency of traditional wireless audio acquisition and transmission design is also tested as baseline. In that system, a Conexant 20751 sound card is used to for sound sampling, a Realtek RTL8723BE WLAN NIC and a Realtek Bluetooth 4.0+ High Speed Chip are used for wireless transmission. We design an audio recording system and test the running time for each audio frame. As for the transmission delay, we rely on the timestamp field of streaming packets in the receiver to calculate the time of flight. Note that the supported data rate of those wireless devices can satisfy the requirement of audio streaming and there will be no additional delay caused by queuing. In our system, the latency comes from the time for capturing spatial audio using PPM or DPPM modulation and the time for backscatter reflection. We use an oscilloscope to directly test the time difference between the analog audio input and the corresponding digital control logic for the RF switch. Results are shown in Fig. 10.9. When audio track count is increased from 1 to 4, the latency rises from 17.2 μs to 87.4 μs in our system. While traditional design needs tens of

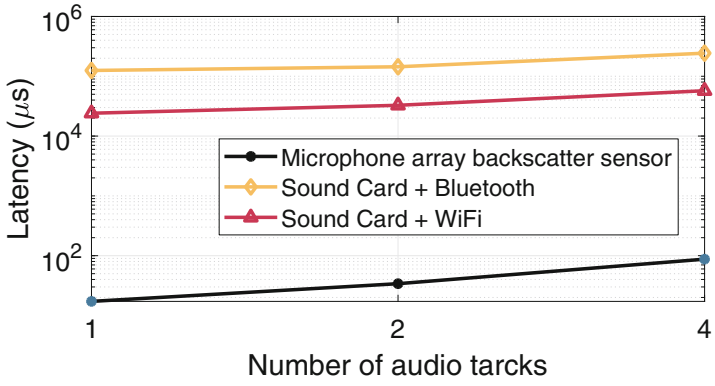


Fig. 10.9 Latency on streaming

milliseconds. For example, the latency times using Wi-Fi and Bluetooth in the setting of 4 tracks are 57.3 ms and 243.2 ms, respectively.

10.4.2.2 Fidelity

Besides the latency, fidelity is another crucial aspect for sound information. The original and regenerated sound waveforms for an audio track in 50 ms are shown in Fig. 10.10. As can be virtually seen that our microphone array backscatter can sample and transmit audio signal and the demodulation design in USRP also works well. We use the Pearson correlation coefficient between original sound waveform and the demodulated one to examine the sound fidelity. As shown in Fig. 10.11, the similarity between the two waveforms decreases when the tag-to-reader distance is increased for SNR drop. We also observe that increasing the analog baseband sample rate for each track results in an improvement in the similarity. The demodulation process depicted in Fig. 10.6 employs lowpass RC filters to recover sound waveform from the PPM baseband. The distortion caused by

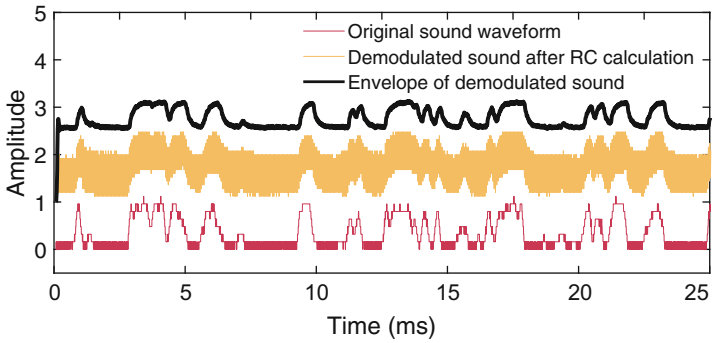


Fig. 10.10 Comparison of original and demodulated sound waveforms

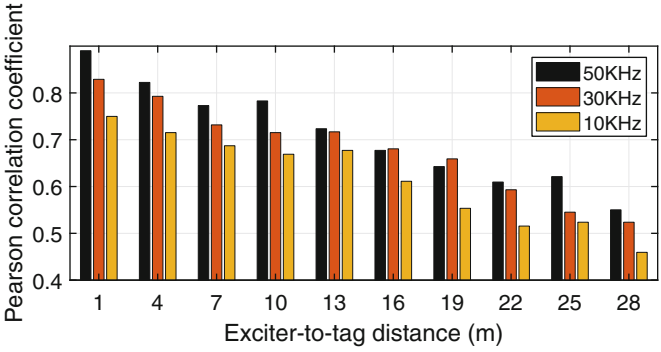


Fig. 10.11 Pearson correlation coefficient testing result

this filter is similar to quantization error and thus can be mitigated by oversampling. Thus, a higher sample rate leads to a more higher similarity to original sound waveform.

10.4.3 Coverage

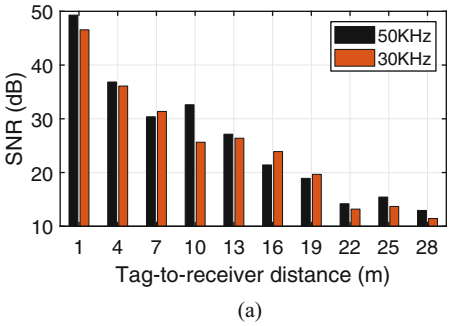
Besides the sound latency and fidelity, the supported working range is also important for the microphone array backscatter system. The backscatter reflection may cause significant SNR drop and influence the decoding range. We investigate the supported exciter-to-tag distance and the tag-to-receiver distance.

10.4.3.1 Tag-to-Receiver Distance

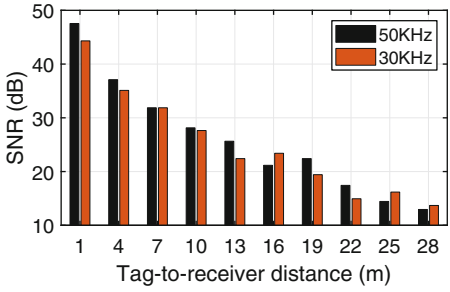
In this section, we evaluate the communication range in an indoor environment. Both line-of-sight and non-line-of-sight scenarios are considered. A USRP N210 together with an HA901I-APC RF amplifier are used to generate an 895 MHz single-tone signal for backscatter excitation. Another USRP N210 device is used to decode the transmitted audio signal. We investigate how the distance, sampling rate, and track count influence the SNR. We place the microphone array backscatter close to the exciter and move the reader away gradually from the sensor. Both PPM and DPPM results are combined.

The line-of-sight results are shown in Fig. 10.12. As shown in Fig. 10.12a, the SNR drops significantly with distance when 4 audio tracks are considered. When tag-to-receiver distance is increased from 1 m to 28 m, the SNR drops from about 50dB to only 10 dB. Similar SNR degeneration also appears when the audio-track count is 8. As mentioned above, the spatial audio data rate equals to the product of sampling rate, track count, and the ADC quantization depth. To support the 8-track, 16-bit resolution sound with 50 kHz sampling rate, our microphone array backscatter reaches an equivalent throughput of 6.4 Mbps.

As shown in the experiment results, the line-of-sight SNR decreases with tag-to-receiver distance. Still, it can be seen that the sampling rate and the audio-track count do not have significant influence on the SNR. During the wireless transmission, the relationship between SNR and sampling rate is different from the ADC sampling procedure. In digital signal processing theory, sampling a signal at higher rate will distribute the quantization noise to a wider spectrum, and the noise density will be reduced. The target signal can be focused on a narrow spectrum band by corresponding processing technique so as to keep high density and boost the SNR. With fixed ADC quantization depth, oversampling can increase the signal to quantization noise ratio (SQNR) and effective number of bits (ENOB). In a word, the tag-to-receiver distance significantly influence the SNR in wireless backscattering. Although the audio track count and the sampling rate only have slight impact on the wireless transmission SNR, they are important for the sampling

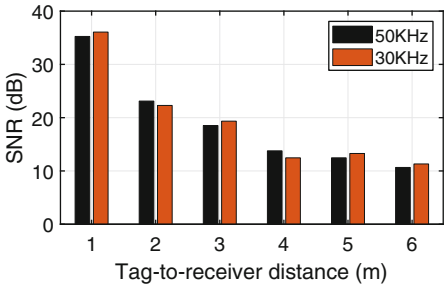


(a)

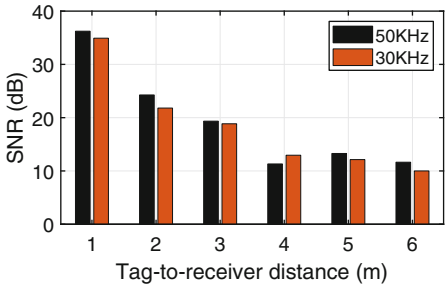


(b)

Fig. 10.12 Light-of-sight backscatter SNR testing results. (**a**) 4 audio tracks. (**b**) 8 audio tracks



(a)



(b)

Fig. 10.13 Non-light-of-sight backscatter SNR testing results. (**a**) 4 audio tracks. (**b**) 8 audio tracks

quality and the spatial resolution of audio signal. On the other hand, they also determine the circuit complexity and the power consumption of PPM and DPPM baseband circuits. Higher quality and more audio tracks mean more complex system design and more power consumption. That's a tradeoff.

In the non-line-of-sight experiment scenario, we observe a similar trend where the backscattered signal's SNR decreases with distance. The results are shown in Fig. 10.13. In the setting of 30 kHz sampling rate and 4 audio tracks, the maximum supported range reaches 6 m. At a distance of 1 m, the SNR is as high as 35 dB, and when the distance increases to 6 m, the SNR drops to about 15 dB. For a sampling

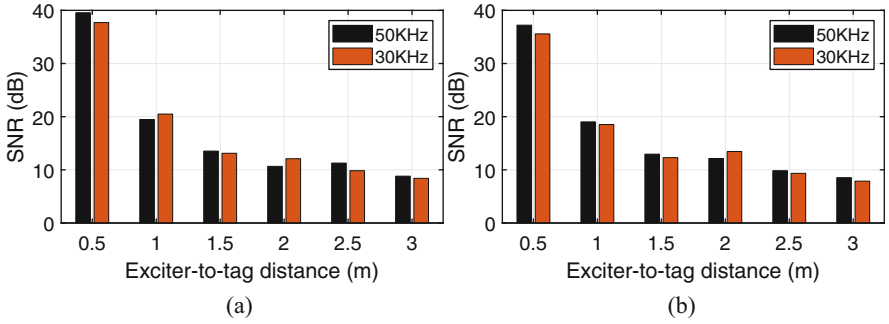


Fig. 10.14 Light-of-sight backscatter SNR testing with exciter-to-tag distance. (**a**) 4 audio tracks. (**b**) 8 audio tracks

rate of 50 kHz or audio track count of 8, we have observed similar experiment results.

10.4.3.2 Exciter-to-Tag Distance

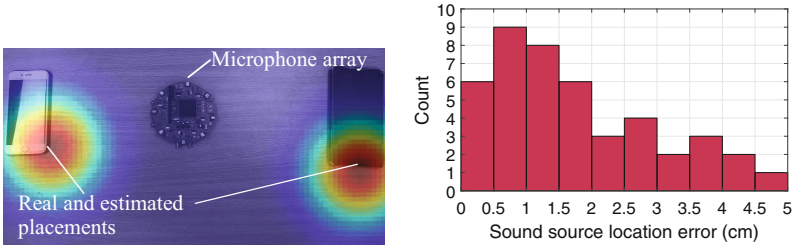
We investigate the influence of the tag-to-exciter distance on the quality of the backscattered signal. The reader is fixed at 1 m away from the backscatter tag, and we move the excitation source to increase the excitation-to-tag distance. The SNR of received signal is shown in Fig. 10.14. The SNR of the backscattered signal deteriorates as the distance increases, and it is not affected by the sampling rate or audio track count. As can be seen that the SNR is only 10 dB with the distance of 3 m. So the excitation source should be placed within a range of 3 m from the sensor to keep a good signal quality.

10.5 Application

Our backscatter system for spatial audio has versatile applications in everyone's daily life, industrial scenarios, and medical treatment. To showcase its potential, we give three application examples.

10.5.1 Acoustic Imaging

The first application case is the acoustic imaging system. We can use the microphone array system design and the corresponding location algorithm to depict the nearby sound strength field, so as to locate the sound source. We use an example to show


Microphone array
Real and estimated placements
Count
Sound source location error (cm)
0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5
0 1 2 3 4 5 6 7 8 9 10

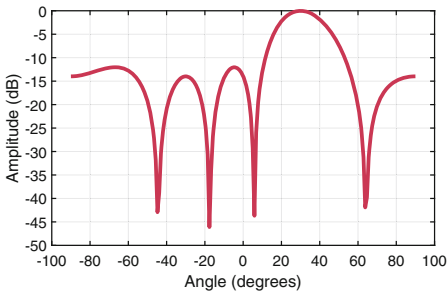
(a) (b)

Fig. 10.15 Acoustic imaging using our system. (**a**) Visualization of real placement and imaging result. (**b**) Precision

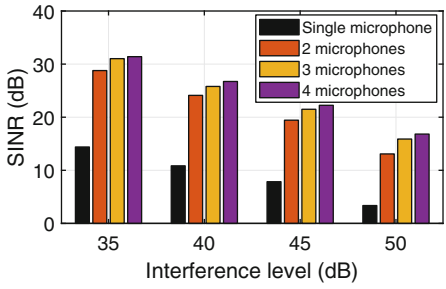
its effectiveness. As shown in Fig. 10.15a, two cellphones are placed close to the microphone array backscatter sensor to work as sound source. The microphone sensor tag samples the spatial sound and then transmits it to the reader. Based on the delay differences of recovered sound waveforms in audio tracks caused by the microphone sensors' spatial positions, a location algorithm is utilized to locate the sound sources. To visualize the sound sources in the area, we used a jet color map to overlap with the placement picture. It can be seen that the imaging results accurately demonstrate the locations of cellphone loudspeakers. Figure 10.15b presents the location error distribution in 44 trials. As can be seen that about 66% of the trials have an error within 2 cm. Such accuracy comes from the much smaller propagation speed and wavelength of sound waveform compared to those of electromagnetic wave in wireless location systems.

10.5.2 Spatial Filtering and Speech Enhancement

Benefiting from the ability of resolving spatial audio, our microphone array backscatter can also be used to enhance directional sound and weaken potential interference in other directions. The mechanism is simple: the microphone sensor closer to sound source will get corresponding sound waveform earlier. By boosting the microphone sensor output at the target direction and weakening sound from other sensors, the directional beamforming can be realized. For example, we can use five microphone sensor to combine an array and realize a beamforming filter with the main lobe width of 30°. The directional pattern is shown in Fig. 10.16a. Our target direction is near 30°, and in this direction, the sound wave will be directly received. If there is still an interference sound source in $-30°$ direction, the corresponding audio signal will undergo an additional attention of about 15 dB. There will be an improvement of about 15dB in the signal-to-interference -plus-noise ratio (SINR). More testing statistics are shown in Fig. 10.16b. We also test the peak signal-to-noise-ratio (PSNR) to evaluate the dynamic range of the received



(a)



(b)

Fig. 10.16 Beamforming and noise reduction for directional audio signal enhancement. (**a**) 30° beamform filter design. (**b**) Signal to interference-plus-noise

signal. Results show that the PSNR drops with the tag-to-receiver distance. When the distance is below 1 m, the PSNR is more than 50dB. To prove the potential of real-world usage in wearable devices and immersive applications, the quality of user experience is also paramount. We assess the subjective quality of single-track and multi-track audio using a five-grade scale (1: Bad, 2: Poor, 3: Fair, 4: Good, and 5: Excellent), following ITU's recommendation [52]. Users listen to the beamformed audio and compare it with the reference sound, then give their experience score. In the testing, such attributes including transparency, timbre, echoes, harmonic distortion, quantization error, and background noise are considered. For single-track audio, an average quality score of 3.62 is achieved. For multi-track audio that mainly focused on the subjective impression of stereophonic or spatial effects (e.g., the relative position of multiple sound sources), the average score is 3.37. Note that the beamforming is a total software solution, and the microphone array backscatter just needs to do PPM or DPPM baseband sampling. No additional operation is needed.

10.5.3 Ultrasonography

Besides the spatial audio recording, our system design including the PPM or DPPM circuits and the backscatter transmission can also be used in ultrasound imaging to help medical diagnosis. The only modification should be made to current prototype

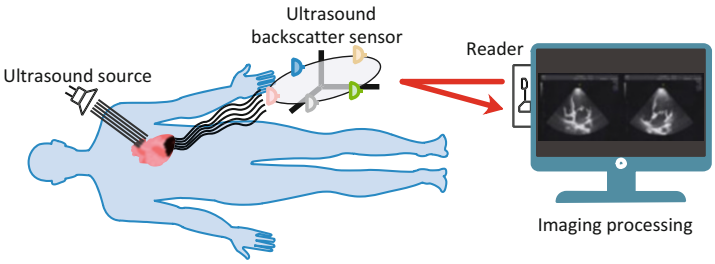


Fig. 10.17 Ultrasound imaging: B-scan for heart diseases

is replacing the microphone sensors with those supporting ultrasound. Ultrasound has a frequency higher than 20 kHz, and its frequency bandwidth can be much larger than the sound acceptable to human ears. The higher frequency means shorter wavelength, which leads to more focused beam and higher azimuth resolution in imaging [53, 54]. Still, the larger bandwidth means better discernibility in distance dimension. Combining two aspects, a much smaller error can be achievable comparing the 2 cm error of sound imaging. This makes our system design suitable for the medical diagnosis. For example, as shown in Fig. 10.17 it may be used in the B-scan ultrasonography. The low latency, multiple-track ability, high fidelity, and light-weight design will help improve service.

10.6 Discussion

Compatibility Our microphone array backscatter supports a equivalent throughput as high as 6.4 Mbps with 8 audio tracks, which is competitive in existing backscatter systems. But we still need the single-tone excitation. There is still some difficulty to make the backscattering part compatible with COTS radios. On the one hand, excitations from commercial devices are intermittent in time and may cause higher latency in the spatial audio. On the other hand, accurate synchronization between microphone array backscatter tag and the exciter still needs to be realized [23, 35, 38].

Eavesdropping Security design has not been included in our system. Existing encryption solutions usually cause high computation burden and thus not suitable for microphone array backscatter sensor. In fact, how to resist malicious behaviors such as covert listening remains an urgent problem in most backscatter systems. The acoustic-radio transformation technique [6] may be used in our system for eavesdropping. Still, developing light-weight wireless source coding would be another solution.

Operation Range As introduced in Sect. 10.4.3, the maximum tag-to-receiver distance and the maximum exciter-to-tag distance are 28 m and 3 m, respectively.

What's worse, those maximum distances cannot be realized at the same time. For example, when the uplink distance of 28 m, the microphone array backscatter tag is placed close to exciter and the distance is much smaller than 3 m. Such operation range is not satisfactory. Furthermore, we also plan to realize the functions of both exciter and receiver by building a full-duplex reader as done in [55] to simplify deployment. But the supported range will be no more than 3 m. Such performance is not enough in even indoor scenarios. To extend the working range, a natural idea is further boosting the excitation power using the amplifier. But in the ISM band the transmission power is limited for consideration of interference to other radios. The reflection amplifier or the tunnel diode that can boost the reflected signal may be a direction [56].

Energy Harvesting In order to ensure our sensor is self-sustaining, we enable the sensor tag to harvest energy from both sound and Wi-Fi signals. The hybrid harvesting circuit is shown in Fig. 10.18. To collect sound energy, we use the electret microphones to convert sound wave into electrical signal. Then, a conventional diode bridge rectifier extracts a positive DC voltage. After that, we employ a voltage regulator to get a stable direct current (DC) voltage. To collect RF energy from Wi-Fi, we use 2.4 GHz omnidirectional antenna together with a multi-layer chip RF bandpass filter BF2012-L2R4DART/LF to extract the Wi-Fi signal from complex spectrum. Then six-stage Modified Greinacher Rectifier composed of SMS7621 Schottky diodes and capacitors introduced in [57] is utilized to extract and boost the DC voltage from RF Wi-Fi signal. For storage and management of converted energy, an energy harvesting Power Supply LTC3588, a boost charger BQ25505, 25 V $10\,\mu F$ electrolytic capacitors, and LX 0.1F Maxcap double layer storage capacitors are also included in the harvesting module. Testing results show that the harvesting efficiency sound waveform increases with sound signal strength. With sound of 40 dB, 70 dB, 75 dB and 90 dB, the harvested powers are 19.2 μW, 152.5 μW,

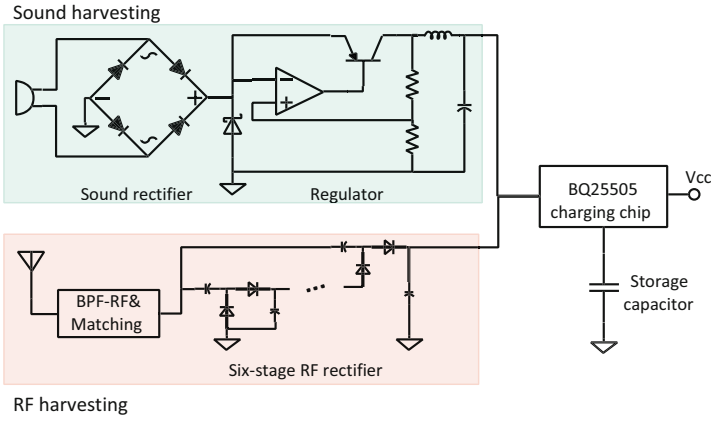


Fig. 10.18 Sound-Wi-Fi energy harvester design

203.6 μW, and 406 μW, respectively. Sound with strength of 70 dB is commonly available in many places including the streets and housing estates, although it is annoying for human beings. 90 dB sound sources exist in the harsh environments, such as the factories and underground trains. According to the energy consumption of the system in Table 10.2, we can get the following conclusions: (1) harvesting the energy from 75dB+ sound can satisfy the requirement in system of PPM baseband; (2) 80 dB sound energy harvesting can satisfy the requirement in system of DPPM baseband with less than 4 tracks; (3) 85 dB sound energy harvesting can satisfy the requirement in system of DPPM baseband with less than 6 tracks; and (4) 90 dB can satisfy the requirement in system of DPPM baseband with at most 8 tracks. For harvesting from Wi-Fi signal, the efficiency also degrades with received signal strength. We use the Qualcomm AR938x NIC as the Wi-Fi signal emitter and test the harvested power with different distance between the harvester and the Wi-Fi transmitter. When the distance ranges from 0.05 m to 1.55 m, the harvested power changes between 85.65 μW and 0.57 μW. They are all lower than the needed power in Table 10.2. In other words, harvesting from Wi-Fi signal alone is not enough to support our microphone array backscatter sensor. One of the key limiting factors is the limited transmission power in Wi-Fi. The Qualcomm AR938x NIC supports at most 18 dBm, which is about 40 times lower than the RFID reader. So, further optimization may be made in the boosting the Wi-Fi power using techniques such as beamforming in MIMO Wi-Fi [28, 38, 44, 58, 59].

Video and Audio Battery-free media has been a hot topic and many systems have been designed. Video streaming is the focus. WISPCam [60–62] introduces embedding commercial camera in RFID-based battery-free sensing and identification platform, WISP, to realize battery-free video streaming. But it can be seen that the camera has a low resolution and its operation causes too much power consumption. For this, high-definition transmission system is designed in [63]. It designs novel analog video modulation and backscattering to fit battery-free scenario and realizes much better video quality with similar power consumption. Its high-level idea is similar to our analog audio modulation. Such similarity provides a chance for design of analog video&audio modulation and transmission.

10.7 Summary

This chapter introduces a novel system that customizes backscatter technique to realize light-weight spatial-audio recording and synchronous wireless streaming. The key enablers are the PPM and DPPM baseband processing. They use roll polling to sample multiple-track audio signals and embed them into one backscatter transmission streaming in specific order, so that the synchronization between audio tracks are kept in nature. Besides low power consumption and simple hardware structure, such design also brings out a high equivalent throughput. The fidelity and latency are both satisfying in the environments. This opens the door for many

advanced applications for both personal usage and industrial or media purpose. For example, the multiple-track audio modulation and streaming technique can be used as the spatial sound recorder in vocal concerts. The voice control application is also a good scenario. The robot can identify the user's location from spatial audio after receiving the voice command "Come here!". Still, our sound modulation design can be combined with the light-weight analog video streaming techniques for such applications as video telephone and VR games. For medical usage, the imaging technique is important in diagnosis of many diseases. Our design enables acoustic imaging and thus has the corresponding application potential. Even further, our analog modulation baseband and backscatter transmission design can be used in ultrasound to realize better imaging accuracy.

References

1. Roy N, Shen S, Hassanieh H, Choudhury RR (2018) Inaudible voice commands: the long-range attack and defense. In: 15th {USENIX} symposium on networked systems design and implementation ({NSDI} 18), pp 547–560
2. Roy N, Gowda M, Choudhury RR (2015) Ripple: Communicating through physical vibration. In: 12th {USENIX} symposium on networked systems design and implementation ({NSDI} 15), pp 265–278
3. Yatani K, Truong KN (2012) Bodyscope: a wearable acoustic sensor for activity recognition. In: Proceedings of the 2012 ACM conference on ubiquitous computing, pp 341–350
4. Tiny-soft-and-wearable-acoustic-sensor. www.printedelectronicsworld.com/articles/10275/
5. Sur S, Wei T, Zhang X (2014). Autodirective audio capturing through a synchronized smartphone array. In: Proceedings of the 12th annual international conference on mobile systems, applications, and services, pp 28–41
6. Wei T, Wang S, Zhou A, Zhang X (2015) Acoustic eavesdropping through wireless vibrometry. In: Proceedings of the 21st annual international conference on mobile computing and networking, pp 130–141
7. Mao W, He J, Qiu L (2016) Cat: high-precision acoustic motion tracking. In: Proceedings of the 22nd annual international conference on mobile computing and networking, pp 69–81
8. Mao W, Wang M, Qiu L (2018) Aim: Acoustic imaging on a mobile. In: Proceedings of the 16th annual international conference on mobile systems, applications, and services, pp 468–481
9. Wang A, Gollakota S (2019) Millisonic: pushing the limits of acoustic motion tracking. In: Proceedings of the 2019 CHI conference on human factors in computing systems, pp 1–11
10. https://physicsworld.com/a/wearable-acoustic-system-monitors-foetalmotion/
11. https://www.gearpatrol.com/tech/a36932143/apple-spatial-audio-vs-dolbyatmos-whats-the-difference/
12. Benesty J, Chen J, Huang Y (2008) Microphone array signal processing, vol 1. Springer Science & Business Media, New York.
13. Mennill DJ, Battiston M, Wilson DR, Foote JR, Doucet SM (2012) Field test of an affordable, portable, wireless microphone array for spatial monitoring of animal ecology and behaviour. Methods Ecol Evol 3(4):704–712
14. https://www.minidsp.com/applications/usb-mic-array
15. www.acoustic-camera.com/en/products/microphone-arrays.html
16. https://facebookincubator.github.io/facebook-360-spatial-workstation/
17. https://www.adobe.io/apis/creativecloud/audition.html

18. Gollakota S, Reynolds MS, Smith JR, Wetherall DJ (2013) The emergence of rf-powered computing. Computer 47(1):32–39
19. Abedi A, Mazaheri MH, Abari O, Brecht T (2018) Witag: Rethinking backscatter communication for wifi networks. In: Proceedings of the 17th ACM workshop on hot topics in networks, pp 148–154
20. Kellogg B, Parks A, Gollakota S, Smith JR, Wetherall D (2014) Wi-fi backscatter: Internet connectivity for rf-powered devices. In: Proceedings of the 2014 ACM conference on SIGCOMM, pp 607–618
21. Bharadia D, Joshi KR, Kotaru M, Katti S (2015) Backfi: High throughput wifi backscatter. ACM SIGCOMM Comput Commun Rev 45(4):283–296
22. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: Bringing low power to wi-fi transmissions. In: 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16), pp 151–164
23. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: Towards internet connectivity for implanted devices. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 356–369
24. Zhang P, Rostami M, Hu P, Ganesan D (2016) Enabling practical backscatter communication for on-body sensors. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 370–383
25. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: Practical backscatter using commodity wifi. In: Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM, pp 259–271
26. Hu P, Zhang P, Ganesan D (2015) Laissez-faire: Fully asymmetric backscatter communication. ACM SIGCOMM Comput Commun Rev 45(4):255–267
27. Hu P, Zhang P, Rostami M, Ganesan D (2016) Braidio: an integrated active-passive radio for mobile devices with asymmetric energy budgets. In: Proceedings of the 2016 ACM SIGCOMM conference, pp 384–397
28. Liu V, Parks A, Talla V, Gollakota S, Wetherall D, Smith JR (2013) Ambient backscatter: wireless communication out of thin air. ACM SIGCOMM Comput Commun Rev 43(4):39–50
29. Parks AN, Liu A, Gollakota S, Smith JR (2014) Turbocharging ambient backscatter communication. ACM SIGCOMM Comput. Commun. Rev 44(4):619–630
30. Talla V, Kellogg B, Ransford B, Naderiparizi S, Gollakota S, Smith JR (2015) Powering the next billion devices with wi-fi. In: Proceedings of the 11th ACM conference on emerging networking experiments and technologies, pp 1–13
31. Zhang P, Ganesan D (2014) Enabling bit-by-bit backscatter communication in severe energy harvesting environments. In: 11th {USENIX} symposium on networked systems design and implementation ({NSDI} 14), pp 345–357
32. Zhang P, Hu P, Pasikanti V, Ganesan D (2014) Ekhonet: High speed ultra low-power backscatter for next generation sensors. In: Proceedings of the 20th annual international conference on Mobile computing and networking, pp 557–568
33. Wang A, Iyer V, Talla V, Smith JR, Gollakota S (2017) Fm backscatter: enabling connected cities and smart fabrics. In: NSDI, vol 17, pp 3154630–3154650
34. Talla V, Kellogg B, Gollakota S, Smith JR (2017) Battery-free cellphone. Proc ACM Interact Mob Wearable Ubiquitous Technol 1(2):1–20
35. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: Backscatter communication using commodity radios. In: Proceedings of the 13th international conference on emerging networking experiments and technologies, pp 389–401
36. Xu X, Shen Y, Yang J, Xu C, Shen G, Chen G, Ni Y (2017) Passivevlc: Enabling practical visible light backscatter communication for battery-free iot applications. In: Proceedings of the 23rd annual international conference on mobile computing and networking, pp 180–192
37. Talla V, Hessar M, Kellogg B, Najafi A, Smith JR, Gollakota S (2017) Lora backscatter: Enabling the vision of ubiquitous connectivity. Proc ACM Interact Mob Wearable Ubiquitous Technol 1(3):1–24

38. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) Plora: a passive long-range data network from ambient lora transmissions. In: Proceedings of the 2018 conference of the ACM special interest group on data communication, pp 147–160
39. Vasisht D, Zhang G, Abari O, Lu H-M, Flanz J, Katabi D (2018) In:-body backscatter communication and localization. In: Proceedings of the 2018 conference of the ACM special interest group on data communication, pp 132–146
40. Naderiparizi S, Hessar M, Talla V, Gollakota S, Smith JR (2018) Towards battery-free {HD} video streaming. In: 15th {USENIX} symposium on networked systems design and implementation ({NSDI} 18), pp 233–247
41. Kotaru M, Zhang P, Katti S (2017) Localizing low-power backscatter tags using commodity wifi. In: Proceedings of the 13th international conference on emerging networking experiments and technologies, pp 251–262
42. Kotaru M, Zhang P, Katti S (2017) Localizing low-power backscatter tags using commodity wifi. In: Proceedings of the 13th international conference on emerging networking experiments and technologies, pp 251–262
43. Hessar M, Najafi A, et al (2019) Netscatter: enabling large-scale backscatter networks. In: Proceedings of the 16th USENIX symposium on networked systems design and implementation (NSDI'19)
44. Jang J, Adib F (2019) Underwater backscatter networking. In: Proceedings of the ACM special interest group on data communication, pp 187–199
45. Talla V, Smith JR (2013) Hybrid analog-digital backscatter: a new approach for battery-free sensing. In: 2013 IEEE international conference on RFID (RFID). IEEE, pp 74–81
46. Zhao J, Gong W, Liu J (2021) Microphone array backscatter: an application-driven design for lightweight spatial sound recording over the air. In: Proceedings of the 27th annual international conference on mobile computing and networking, pp 710–722
47. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of the 16th annual international conference on mobile systems, applications, and services, pp 191–203
48. Zhao J, Gong W, Liu J (2018) X-tandem: Towards multi-hop backscatter communication with commodity wifi. In: Proceedings of the 24th annual international conference on mobile computing and networking, pp 497–511
49. Shiu D-S, Kahn JM (1999) Differential pulse-position modulation for power-efficient optical communication. IEEE Trans Commun 47(8):1201–1210
50. Wong KT (2007) Narrowband ppm semi-'blind'spatial-rake receiver & co-channel interference suppression. Eur Trans Telecommun 18(2):193–197
51. https://www.xilinx.com/products/design-tools/xst.html
52. https://www.itu.int/dms_pubrec/itu-r/rec/bs/R-REC-BS.1284-2-201901-I!!PDF-E.pdf
53. Ng A, Swanevelder J (2011) Resolution in ultrasound imaging. Contin Edu Anaesthesia Critical Care Pain 11(5):186–192
54. Silverman RH (2009) High-resolution ultrasound imaging of the eye–a review. Clin Exp Ophthalmol 37(1):54–67
55. Katanbaf M, Weinand A, Talla V (2021) Simplifying backscatter deployment: full-duplex lora backscatter. In: NSDI, pp 955–972
56. Varshney A, Soleiman A, Voigt T (2019) Tunnelscatter: Low power communication for sensor tags using tunnel diodes. In: The 25th annual international conference on mobile computing and networking, pp 1–17
57. Curty J-P, Joehl N, Krummenacher F, Dehollain C, Declercq MJ (2005) A model for /spl mu/-power rectifier analysis and design. IEEE Trans Circuits Syst I Regul Pap 52(12):2771–2779
58. Ma Y, Luo Z, Steiger C, Traverso G, Adib F (2018) Enabling deep-tissue networking for miniature medical devices. In: Proceedings of the 2018 conference of the ACM special interest group on data communication, pp 417–431
59. http://wisp5.wispsensor.net.
60. Naderiparizi S, Parks AN, Kapetanovic Z, Ransford B, Smith JR (2015) Wispcam: a battery-free rfid camera. In: 2015 IEEE international conference on RFID (RFID). IEEE, pp 166–173

61. Naderiparizi S, Kapetanovic Z, Smith JR (2016) Wispcam: An rf-powered smart camera for machine vision applications. In: Proceedings of the 4th international workshop on energy harvesting and energy-neutral sensing systems, New York, NY, USA, pp 19–22. Association for Computing Machinery.
62. Menon R, Gujarathi R, Saffari A, Smith JR (2023) Wireless identification and sensing platform version 6.0. In: Proceedings of the 20th ACM conference on embedded networked sensor systems, New York, NY, USA, pp 899–905. Association for Computing Machinery
63. Naderiparizi S, Hessar M, Talla V, Gollakota S, Smith JR (2018) Towards battery-free hd video streaming. In: Proceedings of the 15th USENIX conference on networked systems design and implementation, USA, pp 233–247. USENIX Association

Chapter 11
Apollo: Battery-Free Wearable Sweat Monitoring System

Abstract In this chapter we will introduce a new type of wearable sensor device, Apollo. It is a passive device that captures energy from the environment to power itself. Thus, it can continuously monitor the health of the human body. There are three key parts in its design and implementation, which are the ultra-low power Bluetooth backscatter module, the power management module and the sensor array module. With these key guarantees, our device is able to convert RF energy, solar energy and thermal energy from the environment into electrical energy to ensure the continuous work of the device. The sweat data collected by the sensor array can be transmitted to the smartphone at high speed through the backscatter module. Apollo's prototype is integrated on a flexible PCB and the components it uses are also commercially available off-the-shelf. This makes our device easy to implement and wear. Through extensive experimental studies, we demonstrated that Apollo has an error rate of less than 5% in measuring glucose levels in sweat, while consuming 5.8 mW for sensing and 720 pJ/bit for wireless transmission. The above data marked that Apollo is more than 1700 times less powerful than a standard electrochemical workstation and 26 times less powerful than a commercial BLE chipset. The success of Apollo takes us a step forward in our goal to achieve ubiquitous health monitoring, which will have important applications in the medical field.

11.1 Introduction

The main components of sweat include glucose, lactic acid, potassium ions, sodium ions, and chloride. Studies have shown that the levels of these components in sweat correlate with human health conditions. For example, glucose levels help manage diabetic patients; lactate levels can serve as an early warning of stress ischemia; and chloride levels are an important diagnostic criterion for cystic fibrosis of the pancreas. Therefore, sweat monitoring is clinically important for the diagnosis of endocrine metabolic diseases. In order to enable continuous and convenient monitoring of sweat, we need to use a wearable sweat sensor system. Such a sensor

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_11

system should meet the requirements of being wearable, self-powered, and long-range while allowing for effective monitoring of sweat composition.

1. **Wearable**. Wearable sensor systems are small and portable, and are able to continuously monitor the user's health condition in different states without requiring the user keeping in a particular state, which reduces the demands on the user. A reliable wearable system not only has many conveniences in use, but also avoids additional maintenance costs.
2. **Self-powered**. The traditional battery-powered method is very simple, but the battery has a limited capacity and service life. Frequent charging of the device or constant replacement of the battery will bring a lot of additional maintenance costs, while the used battery will also cause serious pollution to the environment. During the charging of the device, the user must stop using the device, and will not be able to continuously monitor their own health. If the device can capture the energy in the environment for self-powered, then all of the above problems can be easily avoided. Therefore, the sweat sensing system should have the ability to capture energy from the environment for power supply and use this energy for sweat sensing and data transmission.
3. **Long-range**. In order to make our sweat sensing system work in more scenarios, it must be able to communicate over long distances. If we use NFC for communication in our sweat sensing system, we must keep the system very close to the smartphone or tablet, otherwise the device will not work. Therefore, in order to reduce the distance limitation, we consider using BLE signal for communication that supports long distance operation. In this way, users can use our devices without keeping a very close distance from the smartphone and can perform other daily activities such as working or exercising.

In order to achieve easier monitoring of human biological indicators, many works have been devoted to achieving the tiny scale of the system and enhancing its usability[1–4]. However, this is not enough, and none of these efforts have achieved the requirements of wearable, self-powered, and long range that sweat sensing systems should have. Therefore, these systems still have limitations and do not allow for more flexible use scenarios.

Backscatter technology offers an appealing combination of low cost and low power consumption, as demonstrated by Radio Frequency Identification(RFID) [5–10]. This technology relies on a carrier provider and a receiver to establish communication, but the good news is that many researchers have managed to use off-the-shelf devices as both carrier provider and receiver [11–18].

We have developed Apollo to meet specific requirements for wearable biochemical sensing. Apollo utilizes a flexible PCB in the form of a wristband making it both wearable and easy to use. Additionally, Apollo is designed to harvest energy from multiple sources, including RF signals, light, and heat, thus enhancing its performance and expanding its potential applications. Even if only one energy is available, it can still work well. In order to ensure long-range communication with

Fig. 11.1 Wearable sweat analyzing system

minimal power consumption, we have integrated Bluetooth backscatter technology into the system. The backscatter module is capable of detecting BLE signals and filtering out other interferences such as Wi-Fi and ZigBee, which share the 2.4 GHz Industrial Scientific Medical(ISM) band. The sensor data is then transmitted to a smartphone via the identified BLE packets. The sensor array is highly sensitive to concentrations of glucose, lactate, K^+, Na^+, H^+, and Cl^-, which can be estimated by measuring the current or voltage generated (Fig. 11.1).

In conclusion, We build a prototype with commercial off-the-shelf components and conduct extensive experiments to show the effectiveness. The three mentioned requirements are all satisfied. With the differential technique and temperature compensation, the glucose concentration is measured with an error rate below 5%. The biochemical sensing and processing circuit consumes only about 5.8 mW. The backscatter module realizes 720 pJ/bit sensor data transmission which is 26 times more efficient than commercial BLE chipsets.

11.2 Related Work

Backscatter communication is an appealing option due to its low power consumption and connectivity. Various works, such as Passive WiFi [19], Interscatter [20], HitchHike [21], FreeRider [22], and X-Tandem [23], have made significant strides towards making backscatter compatible with commercial devices. Backscatter's advantages include its simple structure, small size, and low power consumption, making it suitable for wearable, self-powered, and long-range applications.

In order to be battery-free, we need to use energy from the environment to power the device. The more common ones are RF energy and light energy. WISP [24, 25] uses the energy capture method of RFID. It converts RF energy into electricity by collecting RF energy from a dedicated RF reader, but this dedicated reader is very expensive. PLoRa [26] and Tunnelscatter[27] choose light energy. But light energy is not stable and is limited by the surrounding environment. Therefore, [28] integrates the advantages and disadvantages of multiple energy sources and chooses to use RF energy, light energy, and relatively stable human thermal energy as the energy source at the same time. This is more adaptable to different application scenarios.

11.3 Apollo Design

11.3.1 System Overview

The basic construction of our self-powered human sweat detection system is shown in Fig. 11.2. This system uses a flexible PCB in order to be made into a wristband form for the user to wear. The entire system consists of three main modules: biochemical sensing, backscatter communication, and energy harvesting. The biochemical sensing module consists of a sensor array and a signal processing path, which occupies more than two-thirds of the entire system area. The remaining PCB area is divided into two other modules, where the ratio of the area occupied by the backscatter communication module to the area occupied by the energy harvesting module is approximately three to one. The energy harvesting part consists of three different energy converters: solar panel for solar energy collection, thermoelectric generator (TEG) for thermal energy collection, and rectifier circuit for RF energy collection. We will describe these in detail in a later section.

Our system contains several different modules that each perform their own functions. Ongoing BLE packets are recognized by the backscatter module, which then uses an RF switch to embed the collected sensor data with the BLE packets to communicate. To capture the energy needed for the system to work, the energy harvesting module uses three different energy converters to collect light, thermal and RF energy. The energy is collected and saved in a storage device. Unlike conventional batteries, our system uses a supercapacitor to store the energy collected

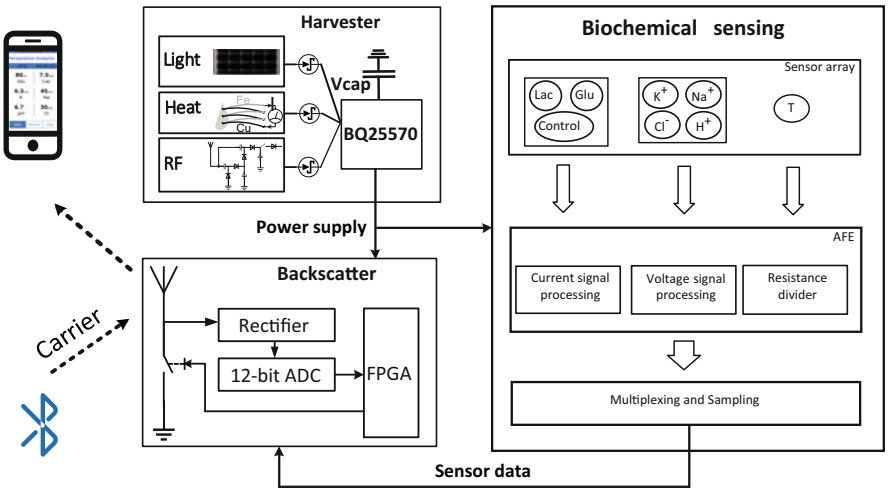


Fig. 11.2 The Apollo biosensor system is comprised of three distinct functional modules, namely the backscatter communication module, the energy harvesting and management module, and the biochemical sensing module

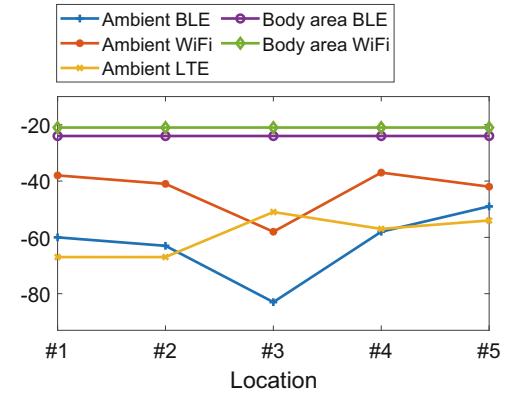
by the system. Finally, our biochemical sensing module collects the levels and concentrations of different components of human sweat, which include lactic acid, glucose, and K^+, Na^+, H^+, Cl^-, etc. Also, the sensor measures the temperature of the sweat. To implement these feeds, the module includes a sensor array, processing path, and multiplexer and ADC for sampling.

When a considerable amount of energy is collected, the biochemical sensing module and backscatter communication module become activated. The low-power FPGA is initially programmed from its non-volatile flash memory and starts functioning. The biochemical sensing module then performs sensor readings across all processing paths, which are managed by the FPGA. The sensor readings are transmitted through backscatter technology, and the packet detection algorithm is executed to recognize any ongoing BLE packets. The tag data modulation module starts transmitting sensor data by toggling the RF-switch as soon as a BLE packet is identified. Following the completion of the modulation, the next cycle of sensor reading and tag transmission commences. This cycle persists until the stored energy becomes inadequate.

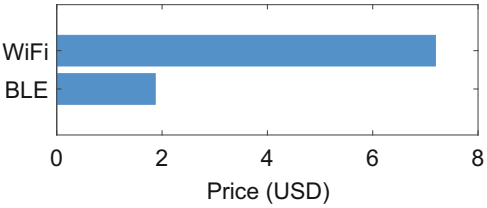
11.3.2 Backscatter Communication

11.3.2.1 Carrier Selection

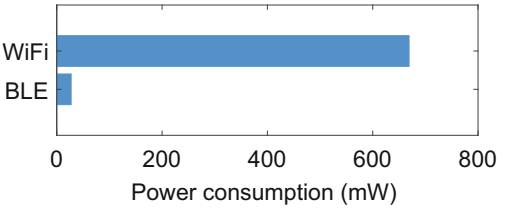
In order to select the appropriate carrier generation device, we focused on Wi-Fi, Bluetooth and LTE, which are common in life. We tested and analyzed the received



(a) Power level of Wi-Fi, BLE, and LTE at campus.



(b) Unit cost.



(c) Power consumption.

Fig. 11.3 RF front for BLE baseband envelope. In (**a**), the Lab, dining hall, playground, classroom, and student dormitory are denoted as locations #1, #2, #3, #4, and #5, respectively. (**b**) and (**c**) depict the unit cost and power consumption of BLE, as compared to Wi-Fi

signal strength indicator (RSSI) of these three signals on campus, and the results are shown in Fig. 11.3a. Observing the experimental results, we found that under indoor conditions, the RSSI of ambient Wi-Fi is about −40 dBm, which is the highest among the three signals, while the RSSI of the other two signals is about 20 dB lower. This pattern is likely to hold in other settings as well. However, since backscatter communication lacks amplifiers, it requires a higher RSSI than ambient signals, which makes these signals unsuitable for this type of communication. Furthermore, after backscatter reflection, the RSSI decreases by over 30 dB[29], resulting in a signal that is too weak and limiting the backscatter range.

In our investigation, we also found that small Bluetooth devices like Bluetooth headsets and smartwatches, they are widely used in some scenarios where they are used in close proximity, so their RSSI at the wrist is as high as −23 dBm "Body area BLE"). In addition, the RSSI of a smartphone held in the hand is able to reach

even higher values. However, considering that BLE has a lower unit cost and lower power consumption compared to Wi-Fi, we believe that BLE is the better choice.

11.3.2.2 BLE Packet Identification

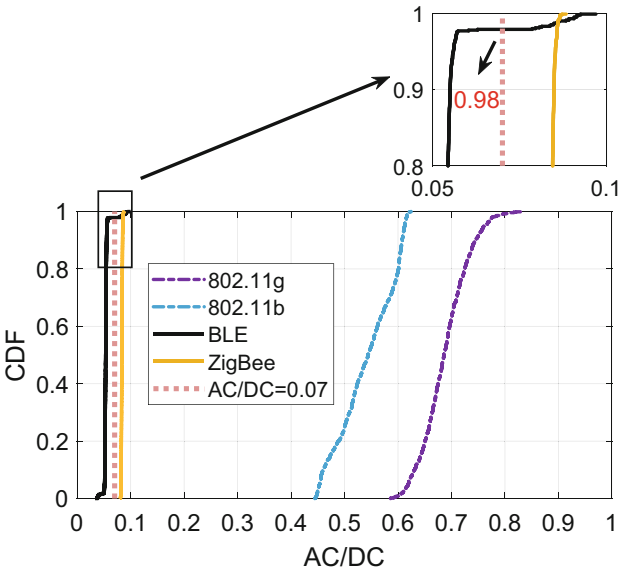
The usual method of detecting packets using active BLE radios involves several energy-intensive steps. First, the received signal from 2.4 GHz ISM frequency band is down-converted to baseband. Then, pulse shaping, carrier frequency offset correction, and cross-correlation with a pre-defined sequence is performed. However, such a processing flow consumes a significant amount of energy, making it unsuitable for our self-powered system. To overcome this challenge, we have adopted a different approach used in WISP and Multiscatter [11, 24]. This method uses a rectifier circuit to obtain the baseband envelope directly, without any additional energy-consuming processing. The baseband envelope can be obtained simply by taking the absolute value of the baseband signal.

The RF rectifier utilizes the characteristic of diodes to quickly charge a capacitor via the diodes during the positive cycle of the signal it received. However, during the negative cycle of the RF signal, the diodes cutoff, and the capacitor discharges slowly. As a result, only the baseband envelope is retained in the output waveform. The extracted BLE baseband contains a dominant DC component, accounting for approximately 99% of the total energy, with the AC component covering only about 1%. In contrast, for 802.11b Wi-Fi and 802.11n Wi-Fi envelopes, the DC components account for about 77% and 47% of the energy, respectively, due to their different bandwidths and modulation schemes. To distinguish between the DC and AC components in real-time, a sliding window of size w is used. The DC component at time instant p is calculated using $D(p) = \frac{\sum_{i=0}^{w-1} V_{base(p-i)}}{w}$, where $V_{base}(p)$ is the sampled envelope data, while the AC component is calculated as $A(p) = V_{base}(p) - D(p)$. The ratio of AC and DC is simplified as the value of

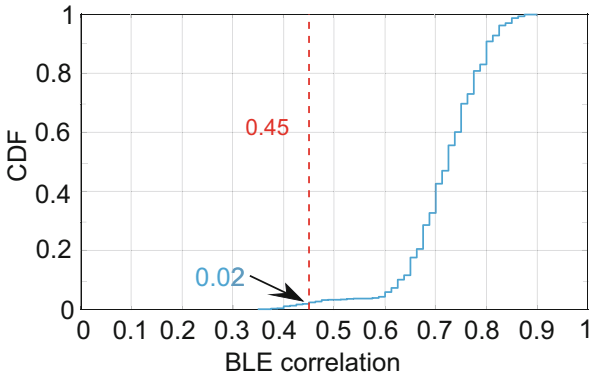
$$AC/DC = \frac{\sum_{p=1}^{L} |A(p)|}{\sum_{p=1}^{L} D(p)} \tag{11.1}$$

where L is the number of points used for BLE packet detection, corresponding to the time duration of BLE preamble and access address. The AC/DC value for BLE packets is typically below 0.06, whereas for Wi-Fi, it is much larger, above 0.4. ZigBee, which is less commonly deployed but also shares the 2.4 GHz ISM band, has an AC/DC value slightly greater than that of BLE. These findings suggest that BLE packets can be differentiated from other commercial packets in the 2.4 GHz ISM band using the AC/DC ratio. The results are depicted in Fig. 11.4a.

To eliminate interference from Wi-Fi and ZigBee packets in BLE signals, the AC/DC method can be employed. However, to validate the presence of BLE packets, it is necessary to conduct a cross-correlation between $A(p)$ and a pre-stored sequence $S(p)$. The DC component $D(p)$ is excluded since it can be treated



(a)



(b)

Fig. 11.4 BLE packet identification. (**a**) Average of *A(p)/D(p)*. (**b**) Correlation with BLE template

as a constant signal, and its cross-correlation with other sequences is of minimal contribution to identifying BLE packets.

In order to simplify the cross-correlation calculation and reduce computational complexity, we employ the sign of both $A(p)$ and $S(p)$ as shown in the following equation:

$$R(i) = \frac{\sum_{p=1}^{L} sign(A(p-i))sign(S(p))}{\sqrt{\sum_{p=1}^{L} sign(A(p))}\sqrt{\Sigma_{p=1}^{L} sign(S(p))}}$$
$$= \frac{\sum_{p=1}^{L} sign(A(p-i))sign(S(p))}{L} \quad (11.2)$$

This simplification allows for 1-bit addition in the cross-correlation calculation, which can be implemented using low-power FPGA. Our experimental results, based on 1000 packets collected in the lab, demonstrate that over 98% of the packets have a cross-correlation greater than 0.45, even in the presence of ambient signals with RSSI below −40 dBm (as shown in Fig. 11.4b). We use a combination of AC/DC and cross-correlation methods to identify BLE packets. Specifically, a packet is identified as BLE if AC/DC is lower than 0.07 and the cross-correlation result is greater than 0.45. We have two methods for detecting BLE packets: the first method involves using only the cross-correlation, identifying the packet as BLE if $R > Th_1$, where Th_1 is a threshold used to filter out interference packets. The second one involves combining cross-correlation and AC/DC. The packet is identified as BLE only if $R > Th_2$ and $AC/DC < Th_3$, and false detections can be controlled by setting thresholds Th_2 and Th_3.

When a BLE packet is detected, the backscatter uses the "Codeword Translation" technique from FreeRider [22] to transmit data. In BLE packets, frequency encodes the information, with f_0 representing bit '0' and f_1 representing bit '1'. When the sensor data is bit '0', the backscatter induces a frequency shift to produce a transition between f_0 and f_1 in the excitation packet, resulting in a change in the information bit. However, when the tag data is bit '0', no codeword translation is performed, and the information contained in the packet remains unaltered. By comparing the decoded data bits with the original bits, the receiver can recover the tag bits using this method.

11.3.3 Power Management

Using energy sources in the environment such as light, vibration, thermal energy, wind, radio-frequency signals, and other available energy sources can serve as a practical alternative to batteries. These energy sources are readily available in the surrounding environment. For example, sources of light like sunlight, lamps, and computer screens, can be utilized for harvesting light energy. Meanwhile, the human body can serve as a natural and consistent thermal energy source, and the increasingly prevalent commercial radios such as Wi-Fi, BLE, and LTE devices, can be a potential source of RF energy. The process of harnessing light energy, thermal energy, and RF energy can be achieved through the use of a solar panel, a TEG, and a rectifier consisting of diodes and capacitors, respectively.

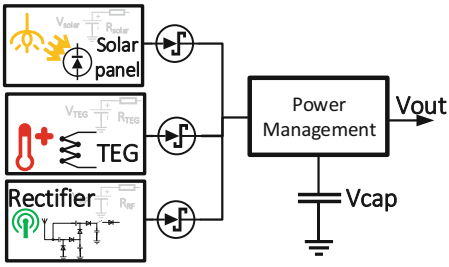


Fig. 11.5 Energy harvester

11.3.3.1 Comprehensive Use of Three Energy Sources

The solar panel, TEG and rectifier we used exhibit different characteristics when collecting light, thermal and RF energy. The resistances of the three collection devices are 6.12 Ω, 119 kΩ, and 1.09 MΩ when the conditions are 10°C, 500 Lux light, and 0 dBm RF signal, respectively. it can be seen that the resistance of the TEG is much lower than the other two. Nevertheless, the voltage that TEG can generate under this condition is only about 0.31 V, while the other two energy sources can generate more than 1.5 V.

To aggregate these three energy sources, we use TI's energy management chip BQ25570. If the device is connected directly to the chip, the TEG will behave as a load, causing much energy to be dissipated. When only solar energy is collected, the other two devices are equivalent to being connected in parallel and acting as loads at the same time. Since the resistance of the TEG is much lower than the other parallel connected devices, it will consume most of the energy and cannot successfully complete the energy collection.

To avoid these problems, we need to adopt a special connection method. Since the system is passive, we cannot use complex control devices and instead we use diodes. Using the single conduction characteristic of the diode, we can isolate the device from the chip as shown in Fig. 11.5. In this way, we can guarantee a high equivalent resistance, so that more energy is delivered to the power management chip.

11.3.3.2 Charging and Discharging

The system performs BLE packet detection, sweat analysis, and backscatter transmission, resulting in a power usage of around 20 mW. To ensure the system operates properly, we use the TI power management chip BQ25570. The system can either stay active as long as there is sufficient stored energy or shut down to allow for quick charging of the storage capacitor.

There are four different states determined by the voltage V_{cap} and its rising or dropping edge:

1. *Shutdown:* If V_{cap} falls below V_{cap_uv} during both the rising and falling edges, the BQ25570 chip's operation is compromised, leading to system shutdown. This situation arises when the storage capacitor is charging from zero or when all energy sources are depleted, causing V_{cap} to decline below V_{cap_uv}, and the storage capacitor to charge slowly.
2. *Shutdown&Charging:* Provided that V_{cap} is within the range of V_{cap_uv} and V_{cap_ready} during the rising edge, or within the range of V_{cap_uv} and V_{cap_ok} during the dropping edge, the system enters a state of shutdown, and the storage capacitor receives a standard charge from the harvested energy. In the absence of any available energy source, V_{cap} will proceed to decrease, while it will increase if there is a source of available energy.
3. *Active&Charging:* If V_{cap} falls between the values of V_{cap_ready} and V_{ov} during the rising edge, or between the values of V_{cap_ok} and V_{cap_ready} during the dropping edge, the system is operational and engages in sweat monitoring. The storage capacitor undergoes regular charging, but in most cases, V_{cap} experiences a rapid decrease due to system consumption. However, if the energy sources are too powerful and the amount of harvested energy exceeds the system's consumption, V_{cap} will continue to increase.
4. *Active:* If V_{cap} is greater than V_{cap_ov} in both rising and dropping edges, the system is active, but charging is stopped to protect the storage capacitor.

Typically, the system alternates between the charging procedure and the discharging procedure with regard to the capacitor voltage V_{cap}. The energy that can be utilized in one complete charging and discharging cycle is given by

$$E_c = \frac{1}{2} C_{store} V_{cap\_ready}^2 - \frac{1}{2} C_{store} V_{cap\_ok}^2. \tag{11.3}$$

Whenever the power supply is restored, the system employs the energy of E_c to transmit and receive sensor data.

11.3.4 Energy-Efficient Sweat Sensing

In this section, we present a method for detecting human sweat efficiently. Our Apollo system includes a specialized biochemical sensor array and signal processing circuits to achieve this goal. The sensor array is designed to detect glucose and lactate by utilizing modified working electrodes with glucose oxidase and lactate oxidase, respectively. For detecting Na^+, K^+, H^+, and Cl^-, we use ion-selective electrodes. The chemical reactions produce either a current signal (for glucose and lactate) or a voltage signal (for Na^+, K^+, H^+, and Cl^-), which are proportional to the concentrations. We utilize a signal conditioning analog front end (AFE), as shown in Fig. 11.6, to prepare the electric signal for processing. The processed signal is then sampled and analyzed by the signal processing circuit.

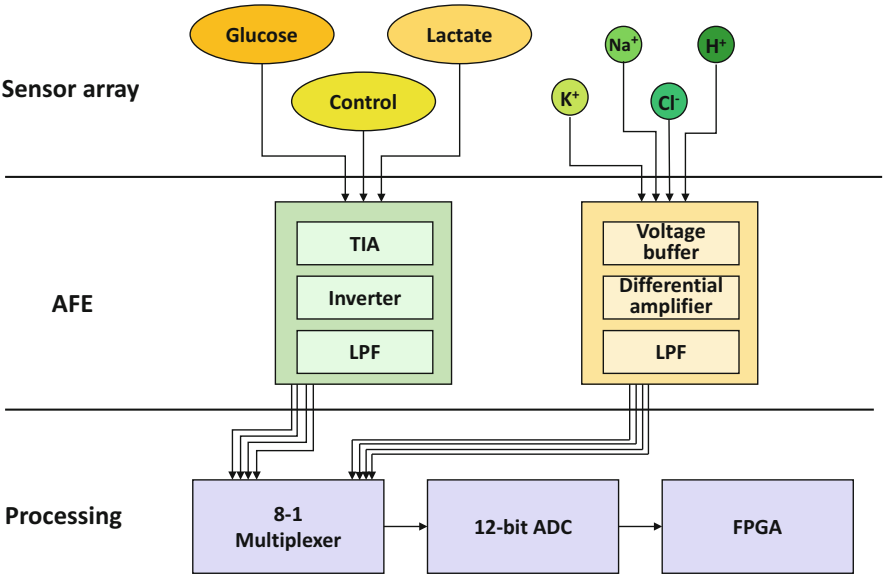


Fig. 11.6 Signal processing paths

We apply a differential measurement method to remove interference from other sweat components. We utilize a reference electrode that lacks glucose oxidase or lactate oxidase, and we calculate the true electric signal as the difference between the working electrode and the reference electrode.

11.4 Performance Evaluation

11.4.1 Implementation Details

Our wearable biochemical system utilizes a flexible printed circuit board designed in a wristband shape, measuring 145 mm × 45 mm, with two layers. The biochemical sensor electrodes are personalized while all the other components are standard commercial-off-the-shelf parts.

11.4.1.1 Backscatter Communication

The present system employs a Microsemi IGLOO nano AGLN250 FPGA as the central control unit for the packet detection algorithm and the RF-switch toggling mechanism. The RF switch, ADG902, is utilized to reflect the RF signal, which facilitates data transmission. To achieve a refined baseband envelope, a

high-bandwidth rectifier, comprising Schottky diodes HSMS-286C, capacitors, and resistors, is employed. The baseband envelope is subsequently sampled by a low-power ADC, the LTC2366. In order to conduct testing and assessment of Wi-Fi (802.11b/n), BLE, and ZigBee packets, laptops equipped with AR938X wireless network adapters, TI CC2540 BLE modules, and TI CC2530 ZigBee modules, respectively, are employed.

11.4.1.2 Energy Harvesting

To harvest different types of energy, we employ various components in our system. Specifically, we utilize a solar cell MP3-37 to capture light energy, six thermoelectric generators TG12-8-01LS connected in series to capture heat energy, and a 5-stage rectifier made up of capacitors and HSMS-286C Schottky diodes to capture RF energy. Additionally, we use the TI BQ25570 to manage charging and discharging, supplying a stable 3.3V DC power output. To address the issue of current leakage and the limited storage capacity of small capacitors, we incorporate a 1000 μF capacitor to store the harvested energy.

11.4.1.3 Sweat Sensing

We construct the signal processing circuit paths using LT1462 operational amplifiers, capacitors, and resistors. To meet the required ± 5 V power rails for the LT1462, we utilize the TPS61220 booster converter to convert the 3.3 V system supply to 5 V. Additionally, we employ the TPS60400 charge pump voltage inverter to generate the -5 V power rail. As previously mentioned, the processed signals for glucose, lactate, K^+, Na^+, H^+, and Cl^- must be sampled by an ADC. To accomplish this, we connect one of these paths to the low-power AD7466 ADC for sensor reading using the ADG758 multiplexer.

11.4.1.4 Power Consumption

The power consumption of our system is around 23.88 mW. This includes 18.08 mW for the backscatter portion and 5.8 mW for the biochemical signal processing circuits.

To demonstrate the power efficiency of backscatter technology, we compared the power needed to transmit one bit of data using backscatter and commercial Bluetooth devices. We used the method described in BLE-backscatter [30] for fairness. Our system consumes 0.18 mW for the RF switch to transmit data at approximately 250 kbps, which is equivalent to 720 pJ/bit. In comparison, the Nordic nRF51822 and TI CC2650 require 18.9 nJ/bit and 18.3 nJ/bit, respectively. Therefore, backscatter technology results in a 26 times power reduction.

Furthermore, the power consumption of the biochemical sensors and signal processing circuits is only 5.80 mW, which is significantly lower than that of electrochemical workstations. For example, CH Instruments, Inc.'s electrochemical workstation model 700E series device consumes tens of Watts.

11.4.2 Evaluation Results

11.4.2.1 Backscatter Communication

1. *Packet detection:* We are currently examining the backscatter communication capability and evaluating the detection rate of BLE packets relative to the sampling rate. To simulate a scenario involving human usage, we used a TI CC2540 BLE module with a maximum RSSI of 4 dBm placed approximately 0.2 m away from the backscatter. We compared the performance of BLE detection using correlation only ($R > Th_1$), or combining correlation and AD/DC ($R > Th_2, AC/DC, Th_2$) while maintaining the false detection rate of other packets, such as Wi-Fi and ZigBee, below 5%.

   Figure 11.7a displays the results of our experiment. We found that both methods achieved detection rates exceeding 90% when the sampling rate was greater than 2.5 MS/s. However, when using cross-correlation only, the detection rate was less than 10% at 1.25 MS/s. Conversely, when combining AC/DC and cross-correlation, the detection rate was still higher than 95% at 1.25 MS/s and higher than 70% at 0.8 MS/s. This represents a significant improvement in detection performance.
2. *Transmission performance:* In a teaching building hallway, we evaluated the throughput over distance by using an amplifier to boost the transmission power to approximately 20 dBm. We provided external power to the backscatter tag, which was placed 0.2 m away from the transmitter. To transmit one bit of backscattered data, we used four carrier symbols of 1 Mbps BLE packets. The results in Fig. 11.7b show the throughput of our system with distance, being able to achieve a maximum operating distance of 17 m. As distance increases, the throughput decreases. However, within 6 m, the throughput remains greater than 200 Kbps, and within 15 m, it remains above 150 Kbps. This level of communication performance is adequate for our sweat monitoring system.
3. *Detection under interference and power efficiency of BLE detection:* We conducted experiments using a Wi-Fi radio to generate 802.11n packets with a payload size of 500 bytes at three different rates: 0 packets per second (no interference), 300 packets per second (low interference), and 1000 packets per second (high interference) as the source of interference. The corresponding BLE detection rates with a sampling rate of 1.25 Msps were depicted in Fig. 11.8a. The decrease in detection rate was due to the collision with Wi-Fi packets.

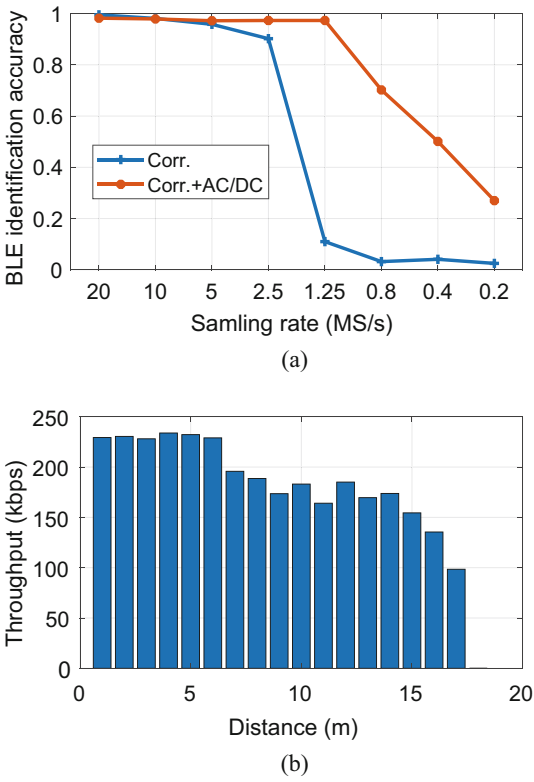


Fig. 11.7 Backscatter communication capability. (**a**) BLE detection accuracy. (**b**) Data rate

The total power consumption was around 23.88 mW. If we only monitor the RSSI to detect carrier packets instead of performing BLE packet detection, the power consumption can be reduced to approximately 17 mW. However, the RSSI method is vulnerable to failure in the presence of Wi-Fi interference, which has a much higher packet rate than BLE (about 30 advertising packets per second). Figure 11.8b illustrates that the failure rate is high when there is low interference, and frequent retransmissions are necessary, resulting in additional power consumption. For instance, with low interference, the failure rate is about 0.865, indicating that a backscatter packet requires an average of 7.4 repeated transmissions. With BLE packet detection, such retransmissions can be avoided, leading to further power savings.

11.4.2.2 Power Harvesting

To demonstrate the effectiveness of using diodes to avoid mutual interference between multiple energy harvesting devices, we tested the charging time with and without diodes for both cases separately. The results in Table 11.1 show that in the

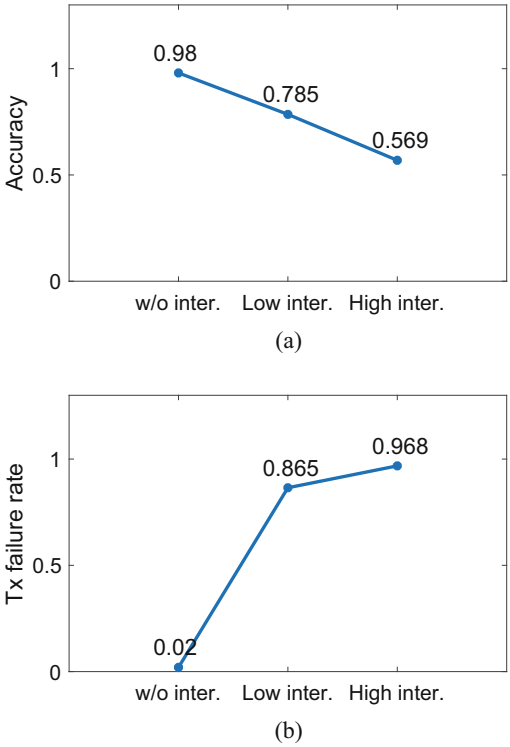


Fig. 11.8 The influence of interference on backscatter transmission. (**a**) Identification accuracy with different interference. (**b**) Transmission failure rate with RSSI method

Table 11.1 Time to charge the super capacitor from V_{cap_ok}(2.60 V) to V_{cap_ready}(4.10 V)

Available energy source	Only available via no diodes	All connected via no diodes	All connected via diodes
500Lux light	21.6 s	–	26.8 s
10°C TEG	3.39 s	3.48 s	5.80 s
6 dBm RF	2.64 s	–	2.84 s

case without diodes, optical and RF energy cannot be successfully collected. In the presence of a diode, all three energies can be successfully collected, but the charging time increases. This is due to the forward voltage of the diode, but it is acceptable compared to being able to collect a wider range of energy.

11.4.2.3 Sweat Sensing and Analyzing

Sweat sensing is significantly affected by temperature, as demonstrated by the example of glucose shown in Fig. 11.9a. As glucose concentration or temperature increases, the response current also increases, leading to ambiguity in glucose measurements. For instance, at a tested current of 3.98 μA, the glucose concentration

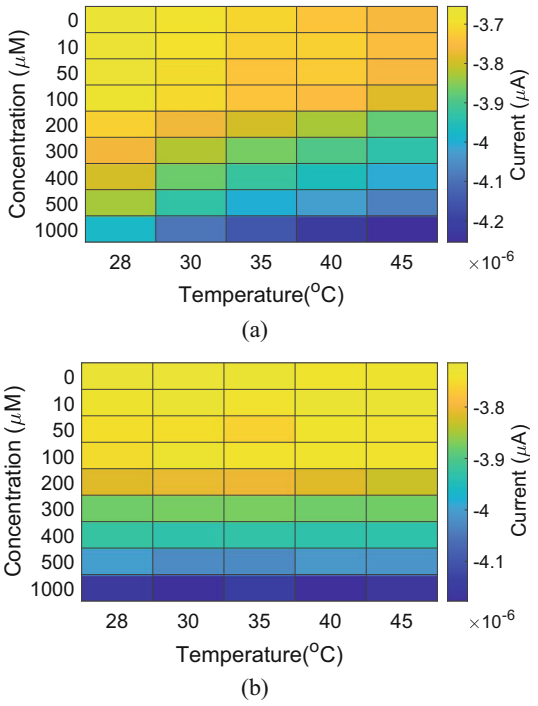


Fig. 11.9 System level real-time temperature compensation for the glucose. (**a**) Without temperature compensation. (**b**) With temperature compensation

may be approximately 1000 μM (at 28°C), 650 μM (at 30°C), or 370 μM (at 45°C), highlighting the influence of temperature on the measurements. To address this issue, we used a 4th order polynomial to compensate for the temperature's effect. As shown in Fig. 11.9b, after compensation, the temperature-induced fluctuations become negligible. In the temperature range from 28°C to 40°C, the error in glucose concentration inferred from the reverse current is less than 5%, which is comparable to the 10% error using a laser [31]. In addition, we measured the sensor temperature in our design using the built-in temperature sensor in the sensor array for compensation.

11.4.2.4 Real-Time Sensor Reading and Data Transmitting

This part of the experimental setup is similar to the previous section, where the performance of the self-system is evaluated by analyzing the energy collected by the system. Figure 11.10 shows that the system is able to obtain effective tag packet rates of 0.733 pkts/s and 36.45 pkts/s when placed under indoor light(500 Lux) or sunlight(104,000 Lux), respectively. At a light intensity of 10,700 Lux, our system is able to perform continuously and can achieve similar performance. In addition, the system can achieve tag packet rates of 1.49 pkts/s and 3.84 pkts/s when using RF energy or thermal energy as the energy source, respectively. Although the harvesting

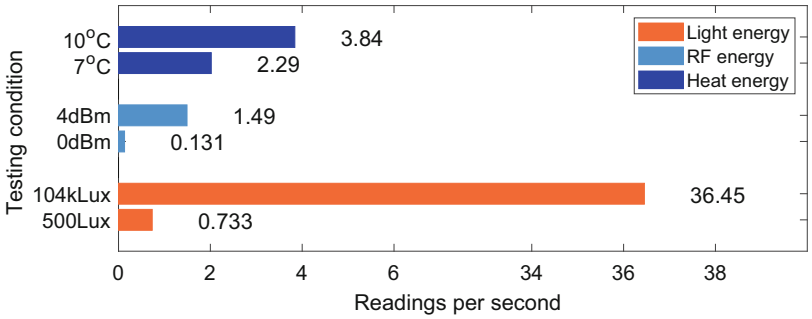


Fig. 11.10 Reading rate with different energy sources

of thermal energy has advantages such as high efficiency and stability, the rigid TEG to be used for harvesting thermal energy needs to be close to the human body, which may cause the user to be unable to perform normal activities. The harvesting of optical and RF energy does not have similar disadvantages, but their acquisition requires some specific conditions. Therefore we combine the harvesting of these energy sources to help expand the use scenarios of the system.

11.5 Application Case

Our sweat monitoring system Apollo is able to analyze the different components of sweat and transmit the results to smart devices, which allows it to be used in many scenarios, such as disease diagnosis and athlete health monitoring.

11.5.1 Disease Diagnosis

In general, a visit to the hospital requires a blood test to analyze the levels of different components in the blood to determine the health of the body. However, the composition of sweat is also closely related to the health of the body. For example, the concentration of glucose in sweat is closely related to whether or not the body has diabetes. Therefore, our sweat monitoring system can be used for disease diagnosis. By analyzing the sensor data received by the smart device, the doctor will be able to know the amount of various components in the patient's sweat and diagnose whether the patient has a certain disease. This not only avoids the need to draw blood, but also shortens the diagnosis time because blood tests are not required.

11.5.2 Athlete Health Monitoring

Athletes tend to sweat a lot during competition, when the sodium ion content in their sweat is much higher than the average level. If water or electrolytes are not replenished in time, it is likely to cause serious health hazards to the athletes. Therefore, athletes can wear our sweat monitoring system to know their situation in real time and adjust their water and salt balance in time. At the same time, by monitoring the athletes' sweat, we can also understand the athletes' health condition before the competition and avoid the athletes from competing with diseases.

11.6 Summary

The Apollo biosensor system is presented in this chapter, which can harvest various ambient energies, monitor human sweat, and transmit sensor readings up to a distance of approximately 17 m. This wearable sensor system is unique in that it incorporates backscatter communication and biochemical sensing technology, making it the first of its kind as far as we are aware.

References

1. Nemiroski A, Christodouleas DC, Hennek JW, Kumar AA, Maxwell EJ, Fernández-Abedul MT, Whitesides GM (2014) Universal mobile electrochemical detector designed for use in resource-limited applications. Proc Natl Acad Sci 111(33):11984–11989
2. Gao W, Emaminejad S, Nyein HYY, Challa S, Chen K, Peck A, Fahad HM, Ota H, Shiraki H, Kiriya D, et al (2016) Fully integrated wearable sensor arrays for multiplexed in situ perspiration analysis. Nature 529(7587):509–514
3. Yang Y, Song Y, Bo X, Min J, Pak OS, Zhu L, Wang M, Tu J, Kogan A, Zhang H, et al (2020) A laser-engraved wearable sensor for sensitive detection of uric acid and tyrosine in sweat. Nat Biotechnol 38(2):217–224
4. Xu G, Cheng C, Liu Z, Yuan W, Wu X, Lu Y, Low SS, Liu J, Zhu L, Ji D, et al (2019) Battery-free and wireless epidermal electrochemical system with all-printed stretchable electrode array for multiplexed in situ sweat analysis. Adv Mater Technol 4(7):1800658
5. Liu H, Gong W, Miao X, Liu K, He W (2014) Towards adaptive continuous scanning in large-scale rfid systems. In IEEE INFOCOM 2014-IEEE conference on computer communications, pp 486–494. IEEE (2014)
6. Liu H, Gong W, Chen L, He W, Liu K, Liu Y (2014) Generic composite counting in rfid systems. In 2014 IEEE 34th international conference on distributed computing systems. IEEE, pp 597–606
7. Gong W, Liu J, Yang Z (2016) Fast and reliable unknown tag detection in large-scale rfid systems. In Proceedings of the 17th ACM international symposium on mobile ad hoc networking and computing, pp 141–150
8. Liu K, Ma Q, Gong W, Miao X, Liu Y (2014) Self-diagnosis for detecting system failures in large-scale wireless sensor networks. IEEE Trans Wirel Commun 13(10):5535–5545

9. Gong W, Stojmenovic I, Nayak A, Liu K, Liu H (2015) Fast and scalable counterfeits estimation for large-scale rfid systems. IEEE/ACM Trans Netw 24(2):1052–1064
10. Gong W, Liu J, Yang Z (2017) Efficient unknown tag detection in large-scale rfid systems with unreliable channels. IEEE/ACM Trans Netw 25(4):2528–2539
11. Gong W, Yuan L, Wang Q, Zhao J (2020) Multiprotocol backscatter for personal iot sensors. In Proceedings of the 16th international conference on emerging networking experiments and technologies, pp 261–273
12. Zhao J, Gong W, Liu J (2018) Spatial stream backscatter using commodity wifi. In: Proceedings of the 16th annual international conference on mobile systems, applications, and services, pp 191–203
13. Gong W, Liu H, Liu J, Fan X, Liu K, Ma Q, Ji X (2018) Channel-aware rate adaptation for backscatter networks. IEEE/ACM Trans Netw 26(2):751–764
14. Zhao J, Gong W, Liu J (2018) X-tandem: Towards multi-hop backscatter communication with commodity wifi. In Proceedings of the 24th annual international conference on mobile computing and networking, pp 497–511
15. Gong W, Chen S, Liu J, Wang Z (2018) Mobirate: Mobility-aware rate adaptation using phy information for backscatter networks. In IEEE INFOCOM 2018-IEEE conference on computer communications. IEEE, pp 1259–1267
16. Gong W, Chen S, Liu J (2017) Towards higher throughput rate adaptation for backscatter networks. In 2017 IEEE 25th international conference on network protocols (ICNP). IEEE, pp 1–10
17. Zhao J, Gong W, Liu J (2020) Towards scalable backscatter sensor mesh with decodable relay and distributed excitation. In Proceedings of the 18th international conference on mobile systems, applications, and services, pp 67–79
18. Wang Q, Yu J, Xiong C, Zhao J, Chen S, Zhang R, Gong W (2020) Efficient backscatter with ambient wifi for live streaming. In GLOBECOM 2020-2020 IEEE global communications conference. IEEE, pp 1–6
19. Kellogg B, Talla V, Gollakota S, Smith JR (2016) Passive wi-fi: bringing low power to wi-fi transmissions. In Proceedings of the 13th usenix conference on networked systems design and implementation, NSDI'16, pp 151–164
20. Iyer V, Talla V, Kellogg B, Gollakota S, Smith J (2016) Inter-technology backscatter: towards internet connectivity for implanted devices. In Proceedings of the 2016 ACM SIGCOMM conference, SIGCOMM '16, pp 356–369
21. Zhang P, Bharadia D, Joshi K, Katti S (2016) Hitchhike: Practical backscatter using commodity wifi. In Proceedings of the 14th ACM conference on embedded network sensor systems CD-ROM, SenSys '16, pp 259–271
22. Zhang P, Josephson C, Bharadia D, Katti S (2017) Freerider: Backscatter communication using commodity radios. In Proceedings of the 13th international conference on emerging networking experiments and technologies, CoNEXT '17, pp 389–401
23. Zhao J, Gong W, Liu J (2018) X-tandem: Towards multi-hop backscatter communication with commodity wifi. In Proceedings of the 24th annual international conference on mobile computing and networking, MobiCom '18, New York, NY, USA. ACM, pp 497–511
24. Philipose M, Smith JR, Jiang B, Mamishev A, Roy S, Sundara-Rajan K (2005) Battery-free wireless identification and sensing. IEEE Pervasive Comput 4(1):37–45
25. Sample AP, Yeager DJ, Powledge PS, Mamishev AV, Smith JR (2008) Design of an rfid-based battery-free programmable sensing platform. IEEE Trans Instrum Meas 57(11):2608–2615
26. Peng Y, Shangguan L, Hu Y, Qian Y, Lin X, Chen X, Fang D, Jamieson K (2018) Plora: A passive long-range data network from ambient lora transmissions. In Proceedings of the 2018 conference of the acm special interest group on data communication, pp 147–160
27. Varshney A, Soleiman A, Voigt T (2019) Tunnelscatter: Low power communication for sensor tags using tunnel diodes. In The 25th annual international conference on mobile computing and networking, pp 1–17

28. Yuan L, Xiong C, Chen S, Gong W (2021) Embracing self-powered wireless wearables for smart healthcare. In 2021 IEEE international conference on pervasive computing and communications (PerCom). IEEE, pp 1–7
29. Dobkin D (2012) The rf in RFID: uhf RFID in practice. Newnes
30. Ensworth JF, Reynolds MS (2017) Ble-backscatter: Ultralow-power iot nodes compatible with bluetooth 4.0 low energy (ble) smartphones and tablets. IEEE Trans Microwave Theory Tech 65(9):3360–3368
31. Li T, Bai D, Prioleau T, Bui N, Vu T, Zhou X (2020) Noninvasive glucose monitoring using polarized light. In Proceedings of the 18th conference on embedded networked sensor systems, pp 544–557

Part V
Future Directions

Part V points out critical challenges for realizing the vision of pervasive backscatter IoTs and potential directions of ambient backscatter applications.

Chapter 12
Challenges and Applications of Pervasive Backscatter

Abstract This chapter points out critical challenges for realizing the vision of pervasive backscatter IoTs and potential directions of ambient backscatter applications. We provide interesting ideas and motivate the reader to use, research, or apply pervasive backscatter technologies in a world of inter-connected smart things.

12.1 Urgent Challenges

Although pervasive backscatter has attracted much attention from academia and industry and has promising prospects, there are still several challenges to be solved.

1. **Protocol compatibility.** Figure 12.1a shows the challenges of protocol compatibility. Network protocols are some specifications for transmitting and managing information in the network (including the Internet). Just like the mutual communication between people needs to follow certain rules, the mutual communication between computers needs to abide by certain rules. These rules are called network protocols. We know that any communication method needs to follow the corresponding standards, and these communication devices used in daily life need to communicate with each other according to the protocol. Therefore, there must be an agreement before the device. For example, base stations that can be seen everywhere in life run in accordance with LTE and 5G protocols. To reduce production cost and deployment complexity, backscatter should reuse existing commercial facilities, such as base stations and mobile phones, which means backscatter communication should be protocol compatible. However, due to the complexity of the protocol and the limited resources of backscatter devices, some existing backscatter devices only implement simple backscatter modulation, and as a result, protocol compatibility has to be sacrificed, especially for LTE, NB-IoT and 5G, etc. Some backscatter works, such as LScatter [1], in pursuit of high throughput, destroy the LTE frame structure and make it impossible for standard LTE UEs to demodulate backscattered signals. The purpose of backscatter is to replace high-power active radios. Therefore, it should not only achieve low power consumption, but also conform to protocol specifications and

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

W. Gong et al., *Pervasive Ambient Communication for Internet of Things*,
https://doi.org/10.1007/978-3-031-38044-0_12

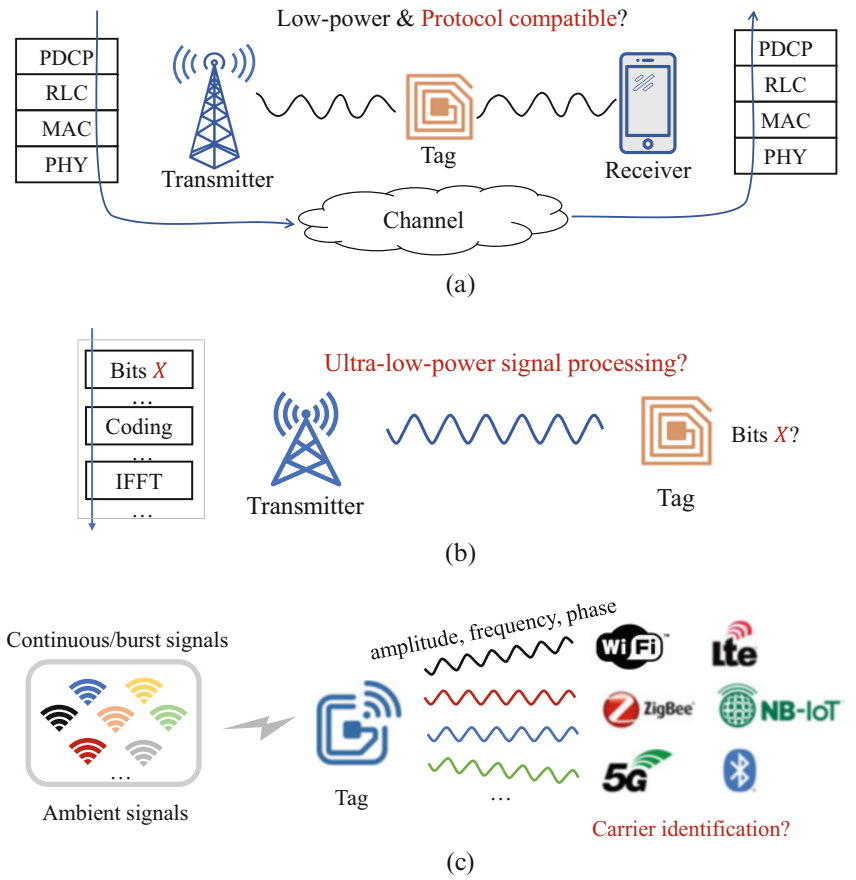


Fig. 12.1 Urgent challenges for pervasive backscatter. (**a**) Protocol compatibility. (**b**) Ultra-low-power signal processing. (**c**) Carrier identification

have its own protocol characteristics. The LTE protocol introduces a paging [2, 3] mechanism with DRX (Discontinuous Reception) [4] to save energy. Similarly, this mechanism can be applied to backscatter, by controlling the backscatter device to switch the power state according to the LTE network traffic conditions to reduce power consumption.

2. **Ultra-low-power signal processing.** Figure 12.1b shows the challenges of ultra-low-power signal processing. The signal processing process is very complicated. For example, OFDM physical layer signal processing includes processes such as synchronization, FFT, and demodulation. For resource-constrained backscatter tags, it is a huge challenge to acquire IQ data from the transmitter because it involves power-intensive operations, such as down-conversion. To ensure ultra-low power consumption, backscatter has to reduce the quality of the sampled data, and an envelope detector is often used to obtain the amplitude of the

excitation signal. Envelope detectors consist of passive components such as diodes, capacitors, and resistors, and are inherently low-power. Due to the limited resources of backscatter tags and the lack of support for high-energy signal processing, it is extremely difficult for ultra-low-power tags to demodulate productive excitation signals. Designing ultra-low power signal processing is quite necessary because it enables tags to have the signal processing capabilities of active receivers. At present, some backscatter works have been carried out towards the direction of demodulation excitation signal, which can backscatter the productive stimulus signal into the native signal received by commercial receivers. Chameleon's [5] attempt to demodulate 802.11b WiFi signals is based on the key observation that phase-modulated 802.11b signals can be distinguished by their pulse width. However, for the demodulation of OFDM signals, there are still huge challenges.

3. **Carrier identification.** Figure 12.1c shows the challenges of carrier identification. There are mainstream radio signals such as WiFi, Bluetooth, and LTE in the environment, and the design that identifies multi-carriers can improve compatibility with sensor devices that support various wireless protocols. Moreover, the multi-carrier identification technology can also make full use of various wireless signals for data transmission, avoiding the communication failure problem of the single-protocol backscatter system in the absence of a carrier, and greatly improving the transmission efficiency. Multiscatter [6] designs multi-carrier identification technology so that backscatter tags can identify various ambient signals including WiFi, Bluetooth and ZigBee. But these radio signals are mainstream indoor signals, and for large-scale deployment, the tags should identify more types of carriers, such as LTE and 5G. However, identification of signals such as LTE and 5G is challenging for two reasons. First, unlike bursty Bluetooth and WiFi signals, LTE and 5G signals are continuous in time; second, the field meta-data used for protocol identification is not at the beginning of the frame. The meta-data of LTE and 5G are primary and secondary synchronization signals (PSS and SSS) located in the middle of the frame, while the meta-data of other signals is often the preamble at the header of the packet. Existing backscatter works use signal's amplitude characteristics to identify the carrier, which has defects such as being interfered with by non-target signals and limited in distance. To solve this challenge, tags can try to accurately identify the carrier from more dimensions, such as frequency. Nevertheless, it is quite challenging for ultra-low-power tags to obtain more dimensional information of the carrier.

12.2 Large-Scale Applications

Finally, we present several potential large-scale applications of pervasive backscatter as shown in Fig. 12.2.

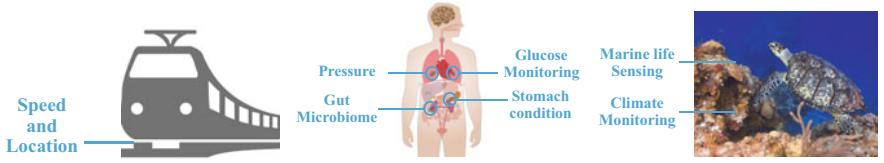


Fig. 12.2 Large-scale applications for pervasive backscatter. (**a**) Trains and subways. (**b**) Wireless drugs. (**c**) Battery-free monitoring

1. **Trains and subways.** With the deployment and development of urban rail transit, more and more people choose bullet trains and subways as their means of travel. To ensure traffic safety, it is very important to accurately locate the train and obtain train information. Traditional train location mainly uses RFID sensing technology, and RFID requires expensive and dedicated readers. With the sharp increase in the demand for train location, the cost of deploying RFID beacons is too high and the deployment difficulty is increased. Pervasive backscatter uses the ambient signal as the carrier, reusing the existing infrastructure to reduce cost and deployment complexity. The tag first perceives the train's speed, location, and other information, and then piggybacks the information on the ambient carrier to the commercial receiver, and finally the receiver demodulates the backscatter signal to obtain the train information.
2. **Wireless drugs.** Today, the monitoring of patients' physiological signs is mainly achieved by attaching sensors to the body surface or implanting the skin, but it has the problem of inaccurate diagnosis. If backscatter can be applied to the human body, it will play a huge role in the medical field. For example, traditional endoscopes need to go deep into the patient's mouth to check the patient's health, which not only brings discomfort to the patient, but also may cause cross-infection. With the development of medicine, the appearance of swallowable capsule endoscope eliminates the pain caused by inserting the traditional endoscope, thus making it easier to examine the gastrointestinal (GI) tract, but it requires a lot of energy and has a limited service life. Backscatter can significantly reduce the power budget of these capsules, allowing them to operate for longer periods of time. Furthermore, if the backscatter signal could be accurately localized, it would allow the capsule to adapt its function according to its position in the GI tract. For example, it could deposit medication in certain areas, or adjust the video frame rate for higher resolution in key areas. Other potential applications of deep tissue backscatter include tracking microrobots in the bloodstream and locating fiducial markers to detect movement of breast, liver, or lung tumors during radiation therapy.
3. **Battery-free monitoring.** There are many unknown creatures in the ocean, and underwater monitoring is an important means of ocean exploration, marine life sensing and underwater climate change monitoring. The current underwater monitoring methods cannot be monitored for a long time due to the limited

battery life of the sensor and the maintenance cost is extremely high. Pervasive backscatter can provide potential opportunities for underwater battery-free monitoring due to its battery-free characteristics. MIT Media Lab has conducted research on underwater backscatter. They proposed that the PAB [7] system enables the underwater network at near-zero power and uses the piezoelectric effect to convert sound energy into electrical energy for underwater backscatter sensing. Nevertheless, it is still extremely challenging for the dynamically changing underwater environment and the depth and transmission rate of the monitoring.

References

1. Chi Z, Liu X, Wang W, Yao Y, Zhu T (2020) Leveraging ambient lte traffic for ubiquitous passive communication. In: Proceedings of the ACM SIGCOMM
2. 3GPP (2018) Evolved universal terrestrial radio access (e-utra); radio resource control (rrc); protocol specification. Technical Specification (TS) 36.331. Version 15.3.0
3. 3GPP (2016) Evolved universal terrestrial radio access (e-utra); user equipment (ue) procedures in idle mode. Technical Specification (TS) 36.304. Version 13.1.0
4. 3GPP (2008) Evolved universal terrestrial radio access (e-utra); medium access control (mac) protocol specification. Technical Specification (TS) 36.321. Version 8.3.0
5. Yuan L, Gong W (2023) Enabling native wifi connectivity for ambient backscatter. In: Proceedings of the ACM MobiSys
6. Gong W, Yuan L, Wang Q, Zhao J (2020) Multiprotocol backscatter for personal IoT sensors. In: Proceedings of the ACM CoNEXT
7. Jang J, Adib F (2019) Underwater backscatter networking. In: Proceedings of the ACM SIGCOMM